# Firewall/VPN Symantec

# Modèles 100 / 200 / 200R

## Guide d'installation et de configuration

Octobre 2001

Le logiciel décrit dans ce manuel est fourni aux termes d'un contrat de licence et ne peut être utilisé qu'en conformité avec ce contrat.

## Copyright



## Marques déposées



Imprimé aux Etats-Unis.

10 9 8 7 6 5 4 3 2 1

# *Table Des Matieres*

## 3. Configuration



## 4. Configuration avancée

# Chapitre 1

# Présentation du produit

La famille de produits Firewall/VPN de Symantec répond à tous les besoins des petites implantations, des bureaux distants, des filiales et des petites entreprises qui souhaitent constituer facilement un réseau et se connecter en toute sécurité à un FAI (fournisseur d'accès à Internet) ou au siège social de l'entreprise. Le Firewall/VPN Symantec protège vos ordinateurs contre les intrusions. La fonctionnalité de Firewall rend votre réseau "invisible" de l'extérieur et rejette toutes les demandes d'informations non autorisés sur votre entreprise.

Le Firewall/VPN Symantec constitue une solution VPN "clé en main" Vous pouvez permettre à votre entreprise de communiquer en toute sécurité en utilisant Internet comme s'il s'agissait de votre réseau d'entreprise privé. Il est ainsi possible aux travailleurs itinérants, aux antennes régionales, aux partenaires et aux revendeurs d'accéder à vos serveurs, tout en garantissant votre sécurité et celle de vos utilisateurs. Le Firewall/VPN Symantec est conçu pour les petites filiales et les agences régionales connectées par DSL, T1 ou des modems câble.

Le Firewall/VPN Symantec vous permet également de partager une connexion Internet large bande entre plusieurs ordinateurs. Vous pouvez l'utiliser pour mettre en réseau tous les PC, imprimantes et serveurs de votre entreprise rapidement et facilement et créer un réseau local. Contrairement à d'autres produits similaires, cette famille de produits fournit les fonctionnalités avancées nécessaires aux entreprises, comme la haute disponibilité intégrée, la connexion de secours automatique et la fonction de VPN (Virtual Private Networking – réseau privé virtuel).

## Firewall - Stateful Inspection

Stateful Inspection fournit une protection contre les pirates, tout en permettant l'accès large bande à Internet. Il prend aussi en charge des fonctions évoluées assurant une grande souplesse de configuration. Le Firewall/VPN Symantec fonctionne avec les firewalls d'entreprise qu'il complète, comme Symantec Enterprise Firewall ou VelociRaptor. Il ne remplace pas les firewalls d'entreprise mais permet de disposer des fonctionnalités appropriées au juste prix.

## Mise en réseau

Le Firewall/VPN Symantec permet aussi de constituer un réseau local. Tous les ordinateurs connectés peuvent ainsi partager des fichiers, des imprimantes et d'autres périphériques réseau. Le commutateur multiport 10/100, en conjonction avec le serveur DHCP intégré, permet à de multiples utilisateurs de se connecter à un réseau partagé avec un simple câble ethernet standard. Le serveur DHCP "loue" des adresses IP aux ordinateurs au fur et à mesure qu'ils se connectent au réseau local. Cette combinaison permet aux utilisateurs les moins expérimentés de mettre un réseau en place rapidement et facilement. La prise en charge de PPPoE est également disponible, ainsi que les fonctionnalités NAT et PAT.

## VPN (Virtual Private Networks - réseau privé virtuel)

La capacité VPN du Firewall/VPN Symantec permet d'établir un tunnel sécurisé et économique entre plusieurs sites, comme le siège social ou le FAI (fournisseur d'accès Internet). Tous les modèles de Firewall/VPN Symantec se comportent comme une passerelle VPN (terminal VPN) pour les tunnels entre passerelles et entre les clients distants et les passerelles (modèle 200R).

## Haute disponibilité / Equilibrage de charge

Les modèles de Firewall/VPN Symantec 200 et 200R comportent deux ports de réseau étendu qui peuvent partager la charge entre les deux ports et même entre deux fournisseurs d'accès Internet utilisant des technologies de connexion différentes (par exemple DSL et le câble).

## Connexion de secours automatique

Les modèles 100, 200 et 200R ont la possibilité de s'interfacer à un modem analogique pour établir une connexion de secours. La fonction de connexion de secours établit automatiquement une connexion à Internet en utilisant le port série si la connexion principale ne fonctionne plus. Vous conservez ainsi un certain niveau de connectivité, même si votre connexion principale à Internet ne fonctionne plus. Cette connexion est automatiquement interrompue quand la connexion principale est de nouveau disponible. Le port série est utilisé pour une connexion analogique ou RNIS, ainsi que pour préconfigurer ou réinitialiser l'unité par l'intermédiaire d'une console de terminal. Le port série peut être utilisé en mode Secours ou comme seule connexion Internet de l'unité en attendant que l'accès Internet large bande soit disponible dans votre région.

## Partage d'adresse IP

La fonctionnalité de Partage d'adresse IP permet à tous les ordinateurs d'un bureau de partager une ou deux adresses IP externes. Ce partage crée de multiples adresses IP internes uniques à partir d'une ou deux adresses IP externes, ce qui permet d'optimiser les coûts de connexion à Internet.

## Consignation – Consignation interne

Le Firewall/VPN Symantec crée un journal local qui enregistre les changements de configuration et les événements liés à la sécurité. Ces journaux sont accessibles à distance par une liaison de gestion cryptée. Le niveau de consignation est configurable.

## Accès à distance

La fonction de Gestion sécurisée à distance permet au FAI ou au siège social d'une entreprise de gérer ces périphériques depuis un emplacement distant. Le Firewall/VPN Symantec peut aussi être géré par l'intermédiaire d'Outils SNMPv1. Ces outils peuvent être téléchargés et existent dans toutes les gammes de prix. Ils permettent de générer des journaux pour fournir une image complète des performances du réseau.

### Connexion directe IPSec/VPN

En plus de créer des tunnels VPN en utilisant le Firewall/VPN Symantec comme terminal, le Firewall/VPN Symantec reconnaît automatiquement les sessions VPN IPSec et leur permet de traverser le firewall. Si vous le souhaitez, vous pouvez autoriser des sessions VPN de clients internes vers des serveurs distants.

### Autres fonctionnalités réseau

Le Firewall/VPN Symantec comporte de nombreuses autres fonctionnalités réseau évoluées pour lui permettre d'évoluer avec vos besoins.

## Fonctionnalités

### Firewall/VPN 100 Symantec

Les fonctionnalités du Firewall/VPN Symantec modèle 100 incluent :

- Quatre ports de réseau local avec commutation 10/100 automatique.
- Un port de réseau étendu 10 Mbits/s.
- Il n'y pas de limitation matérielle au nombre d'utilisateurs mais l'effectif maximum recommandé est de 15.
- Toutes les fonctionnalités énumérées dans la présentation de produit, sauf l'équilibrage de charge et les clients VPN distants.
- Alimentations électriques
- Voyants trafic/connectivité et erreur
- Port série pour connexion de secours automatique par modem
- Micro-commutateurs - Utilisés pour désactiver le serveur DHCP, réinitialiser l'unité, activer la console d'interface série et configurer le Firewall/VPN Symantec pour les mises à niveau du micrologiciel.

- Voyants pour le réseau local - Etat des liaisons 100BaseT, 10BaseT et Duplex pour les ports de réseau local
- Voyant d'alimentation – Allumé quand l'unité est sous tension
- Voyant d'erreur
- Emission/réception sur réseau local et étendu - Allumé quand des données sont transférées entre le réseau étendu et le réseau local
- Voyant de connexion de secours active - Allumé quand la connexion de secours RNIS/analogique est active (quand la connexion large bande est interrompue)

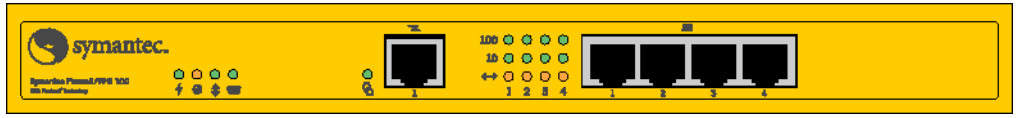



**Figure 1-1 : Panneau avant du Firewall/VPN 100 Symantec**

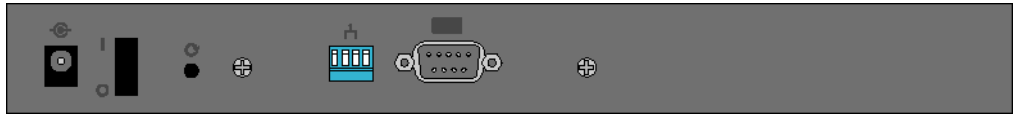


**Figure 1-2 : Panneau arrière du Firewall/VPN 100 Symantec**

## Firewall/VPN 200 Symantec

Les fonctionnalités du Firewall/VPN Symantec modèle 200 incluent :

- Huit ports de réseau local.
- Deux ports de réseau étendu.
- Il n'y pas de limitation matérielle au nombre d'utilisateurs mais l'effectif maximum recommandé est de 30.
- Toutes les fonctionnalités listées dans la Présentation du produit.
- Voyant d'alimentation – Allumé quand l'unité est sous tension.
- Voyant d'erreur.
- Emission/réception sur réseau local et étendu - Allumé quand des données sont transférées entre le réseau étendu et le réseau local.
- Voyant de connexion de secours active - Allumé quand la connexion de secours RNIS/analogique est active (quand la connexion large bande est interrompue).


**Figure 1-3 : Panneau avant du Firewall/VPN 200 Symantec**

**Figure 1-4 : Panneau arrière du Firewall/VPN 200 Symantec**

## Firewall/VPN 200R Symantec

Le Firewall/VPN 200R Symantec dispose de toutes les fonctionnalités du modèle 200. Il est accompagné du logiciel Client Symantec Enterprise VPN, avec firewall personnel intégré.

## Symboles internationaux du Firewall/VPN Symantec

**Table 1-1 : Symboles internationaux du Firewall/VPN Symantec**

| Symbole | Signification |
|---|---|
|  | **Voyant d'alimentation** |
|  | **Voyant d'erreur** |
|  | **Réseau local/réseau étendu**<br>**Voyant de transmission/réception** |
|  | **Voyant de connexion de secours active** |
|  | **Voyant de connexion du modem (réseau étendu)** |
|  | **Port de réseau étendu** |
|  | **Ports de réseau local** |

| Symbole | Signification |
|---|---|
|  | Duplex intégral |
|  | Alimentation |
|  | Réinitialisation |
|  | Allumé |
|  | Eteint |
|  | Micro-commutateur |
|  | Port série |

## Interface de configuration/gestion

Le Firewall/VPN Symantec dispose d'une interface utilisateur basée sur navigateur Web qui permet de créer des configurations, de consulter le statut et d'accéder aux journaux. Les champs de l'interface utilisateur du Firewall/VPN 200 Symantec sont dupliqués pour les deux ports de réseau étendu, sur l'écran de configuration principal comme dans les autres écrans. Cette interface de gestion peut être sécurisée avec la fonctionnalité de VPN intégrée.

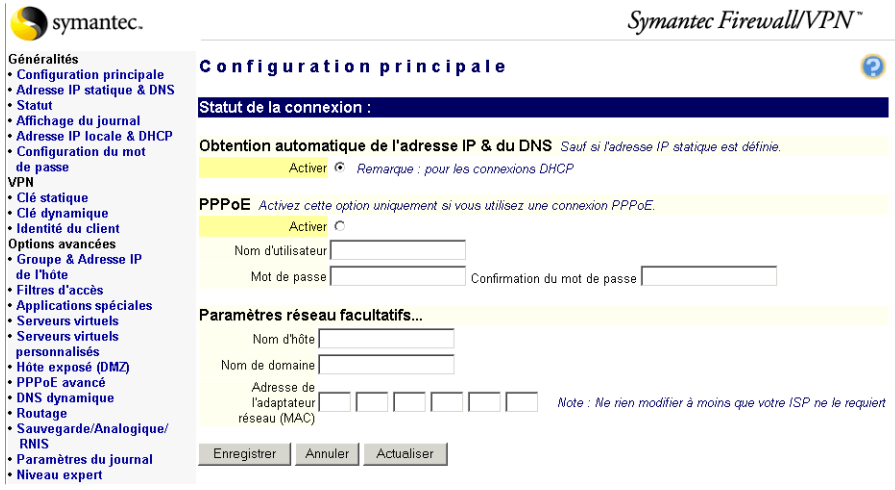



**Figure 1-5 : Exemple d'interface utilisateur du Firewall/VPN 100 Symantec.**

# Chapitre 2

# Installation

## Configuration

L'emballage Firewall/VPN Symantec contient les éléments suivants :

- Unité Firewall/VPN Symantec
- Câble Ethernet CAT5 de 2 m
- CD contenant le manuel d'utilisation, les utilitaires et le Client Symantec Enterprise VPN (200R uniquement)
- Transformateur 9 V CC 1 000 mA
- Carte de démarrage rapide

# Configuration réseau

Vous aurez besoin des éléments suivants pour utiliser le Firewall/VPN Symantec :

- Compte Internet câble ou DSL (ou autre connexion réseau)
- Modem câble ou DSL (ou autre périphérique réseau) avec connexion RJ45 (Ethernet) compatible 10BaseT

  Cet élément est généralement disponible auprès du FAI (fournisseur d'accès Internet) sur simple demande.

- Carte réseau Ethernet compatible 10BaseT ou 100BaseT sur les ordinateurs que vous voulez connecter au Firewall/VPN
- Navigateur Web standard
- Protocole réseau TCP/IP

  Ce protocole est généralement installé dans votre ordinateur et fait partie intégrante de tous les systèmes d'exploitation modernes.

- Câblage UTP (catégorie CAT5) avec connecteurs RJ45 pour connecter les ordinateurs au Firewall/VPN Symantec (un câble est inclus).

# Précautions et avertissements

- Tenez compte de tous les avertissements, notes et instructions indiqués sur le Firewall/VPN.
- Pour protéger l'unité contre les surchauffes, vérifiez qu'elle n'est pas couverte et que la ventilation est suffisante.
- N'utilisez pas et ne stockez pas le Firewall/VPN Symantec dans un environnement dont la température et l'humidité sont hors normes.
- Ne placez pas le Firewall/VPN Symantec près d'un radiateur ou d'une sortie de chaleur si la ventilation appropriée n'est pas assurée.
- Avant de nettoyer le Firewall/VPN Symantec, débranchez-le de la prise murale. N'utilisez pas de nettoyant liquide ni en aérosol. Utilisez un chiffon humide pour le nettoyage.

- Ne placez pas de cordons ou de câbles à un endroit où quelqu'un risque de marcher dessus.
- Veillez à vous conformer à toutes les réglementations ou normes de sécurité locales.
- Des câbles polyvalents sont fournis avec le Firewall/VPN Symantec. Les câbles spéciaux et autres matériels imposés par les réglementations locales sont de la responsabilité de l'utilisateur.
- Les câbles branchés sur des équipements à des emplacements différents, avec des sources d'alimentation et des mises à la terre différentes peuvent présenter des risques d'électrocution. Consultez un électricien qualifié avant d'installer le Firewall/VPN Symantec, pour vérifier s'il existe un problème et prendre les mesures appropriées si nécessaire.
- Ne touchez jamais des fils téléphoniques ou des connecteurs sans débrancher la ligne.
- Evitez d'utiliser un équipement téléphonique ou d'installer le Firewall/VPN Symantec pendant un orage.
- N'installez jamais de prise téléphoniques, de lignes, de câbles réseau, de branchements électriques ou le Firewall/VPN Symantec à un emplacement humide.
- Ne versez jamais de liquide sur le Firewall/VPN Symantec .

# Informations de compte Internet

Pour effectuer l'installation, vous devez déterminer le type de connexion Internet dont vous disposez. Dans le contexte de ce manuel, il peut s'agir de l'un des trois types suivants :

**Compte Internet PPPoE** - La plupart des grands FAI DSL ont adopté cette méthode. Si vous avez un logiciel de "connexion à distance" sur votre ordinateur, vous possédez probablement un compte PPPoE.

- Vous aurez besoin de votre nom d'utilisateur et de votre mot de passe pour installer votre Firewall/VPN Symantec
- Désactivez (ou désinstallez) le logiciel de connexion à distance PPPoE

**Compte Internet DHCP avec IP dynamique** - La plupart des FAI câble, certains DSL.

- Vous n'avez parfois besoin d'aucune information et il suffit de connecter le Firewall/VPN Symantec et de redémarrer l'ordinateur pour être connecté.
- L'adresse MAC (adaptateur réseau) de votre carte Ethernet peut être requise si elle est utilisée par votre FAI (fournisseur d'accès Internet). Vous trouverez plus loin des instructions pour l'obtenir.
- Le nom d'hôte ou de domaine de votre ordinateur peut être requis s'il s'agit d'un nom codé qui vous a été communiqué par votre FAI.

**Compte Internet avec IP statique (ou connexion réseau)**.

- Vous aurez besoin de votre adresse IP, de votre masque réseau et de vos adresses de passerelle et DNS

Certains FAI (généralement câble) utilisent des noms abrégés pour les serveurs de messagerie et les pages d'accueil Web. C'est le cas si le nom de votre page d'accueil Internet est très court, par exemple "www" ou "web" plutôt que www.symantec.com, ou si le nom de votre serveur de messagerie est du genre "pop3" ou "mail" plutôt que mail.symantec.com

Vous DEVEZ disposer des noms de serveur réels pour accéder au Web et à la messagerie en utilisant le Firewall/VPN Symantec. Vous pouvez obtenir ces informations auprès de votre FAI.

# Connexion des câbles

Il est fortement recommandé d'installer votre Firewall/VPN Symantec en lui connectant d'abord un seul ordinateur directement. La résolution d'incidents pendant l'installation en sera grandement facilitée. Une fois l'installation réussie avec un ordinateur, vous pouvez ajouter des ordinateurs ou des concentrateurs au Firewall/VPN Symantec. L'installation suivante illustre cette configuration simplifiée du réseau.

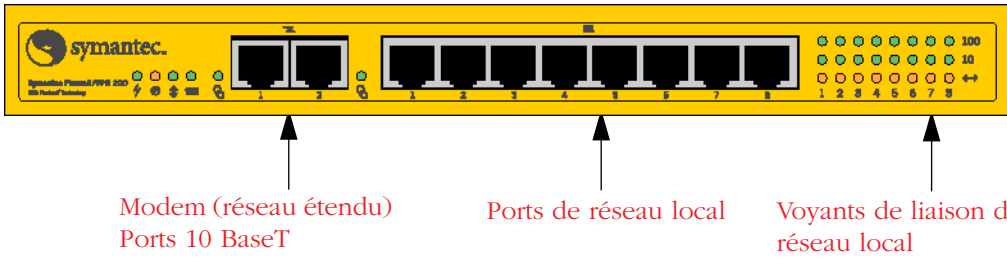



**Figure 2-1 : Panneau avant du Firewall/VPN 200 Symantec**


**Figure 2-2 : Panneau arrière du Firewall/VPN 200 Symantec**

## Pour connecter les câbles

1. Insérez le connecteur du transformateur 9 V DC 1 000 mA fourni avec le Firewall/VPN Symantec et branchez le transformateur dans une prise secteur. Veillez à utiliser EXCLUSIVEMENT le transformateur fourni avec l'unité.

2. Débranchez de l'ordinateur le câble venant (éventuellement) du modem et insérez-le dans le port modem (réseau étendu) du Firewall/VPN Symantec. Le voyant de réseau étendu doit s'allumer en vert. Si ce n'est pas le cas, vérifiez que vous utilisez le même câble que celui du modem.

   Pour le Firewall/VPN 200 Symantec : Répétez cette étape pour chaque port de modem supplémentaire avec un modem ou une connexion séparé (vous pouvez combiner câble, DSL et connexions routées sur les deux ports de modem).

3. Un voyant de liaison vert doit s'allumer sur le voyant de réseau local correspondant. Si ce n'est pas le cas, vérifiez que l'ordinateur est sous tension et que la carte Ethernet fonctionne correctement. Il en est de même pour toutes les connexions établies avec le Firewall/VPN Symantec. Vérifiez toujours qu'un voyant de liaison vert est allumé.

# Configuration de l'ordinateur

La configuration de l'ordinateur implique de définir celui-ci pour qu'il accepte automatiquement l'adressage IP depuis le serveur DHCP du Firewall/VPN Symantec. Cela constitue in réseau interne distinct du réseau externe, doté de son propre système privé d'adressage IP. La procédure de configuration peut varier selon le système d'exploitation de l'ordinateur. Les indications suivantes ne concernent que Windows NT!

Suivez les procédures ci-après pour chaque ordinateur que vous connectez au Firewall/VPN Symantec.

1. Cliquez sur **Démarrer > Paramètres > Panneau de configuration**.
2. Ouvrez **Réseau** et sélectionnez **TCP/IP** (s'il y a plusieurs entrées TCP/IP, choisissez celle liée à votre carte Ethernet).
3. Cliquez sur **Propriétés**.
4. Vérifiez que **Obtenir l'adresse IP automatiquement** est sélectionné.
5. Cliquez sur l'onglet **Passerelle**.
6. Confirmez qu'il n'y a aucune entrée.
7. Cliquez sur l'onglet **Configuration DNS**.
8. Vérifiez que **DNS désactivé** est sélectionné.
9. Si les onglets mentionnés contiennent des entrées, notez celles-ci avant de les effacer, car vous devrez peut-être les fournir au Firewall/VPN Symantec.
10. Redémarrez l'ordinateur.

# Chapitre 3

# Configuration

## Interface de gestion/configuration

Le Firewall/VPN Symantec a une interface de configuration basée Web. Vous pouvez utiliser n'importe quel navigateur Web standard pour configurer les paramètres du Firewall/VPN Symantec. Le menu principal de la gestion/configuration est présent en permanence sur le côté gauche de l'écran.

Les Firewall/VPN Symantec modèle 100 et 200 ont des interfaces légèrement différentes, le modèle 200 comportant deux ports de réseau étendu (modem) dont chacun peut être configuré indépendamment. Le modèle 100 ne dispose que d'un seul port de réseau étendu (modem).

### Pour démarrer l'interface utilisateur

1. Lancez votre navigateur.
2. Si votre navigateur comporte des paramètres de proxy, éliminez ces derniers.

   Si vous ne savez pas comment faire, suivez les instructions suivantes.
3. Saisissez http://192.168.0.1 dans la barre d'adresse de votre explorateur.
4. Appuyez sur la touche **Entrée** du clavier.
5. Le menu principal du Firewall/VPN Symantec s'affiche, comme sur la *Figure 3-1 à la page 3-3*.

### Pour supprimer les paramètres de proxy dans le navigateur Internet Explorer

1. Ouvrez le menu **Outils > Options Internet.**
2. Cliquez sur l'onglet **Connexions**.
3. Cliquez sur **Paramètres LAN**.
4. Décochez toutes les cases et cliquez sur **OK**.
5. Cliquez sur **Ne jamais établir de connexion**.
6. Cliquez sur **OK**.

### Pour supprimer les paramètres de proxy du navigateur Netscape

1. Choisissez **Edition > Préférences.**
2. Cliquez sur **Avancées**.
3. Cliquez sur **Proxies**.
4. Cliquez sur **Connexion directe à Internet.**

## Configuration de base

Les sections suivantes présentent les tâches de base pour la configuration de votre Firewall/VPN Symantec. Une section décrit les fonctions de chaque écran de l'interface utilisateur.

Utilisez l'écran **Configuration principale** pour configurer votre connexion, ou modifier ses paramètres par la suite.

## Ecran Sélection de la langue

Le premier écran affiché après l'installation est l'écran Sélection de la langue. Il n'est affiché qu'une seule fois. Vous pouvez choisir l'une des langues disponibles pour l'interface utilisateur en cochant la case située à côté de la langue. Si vous voulez changer la langue ultérieurement, allez à l'écran Niveau expert, dans lequel ces options sont également disponibles.

# Ecran Configuration principale

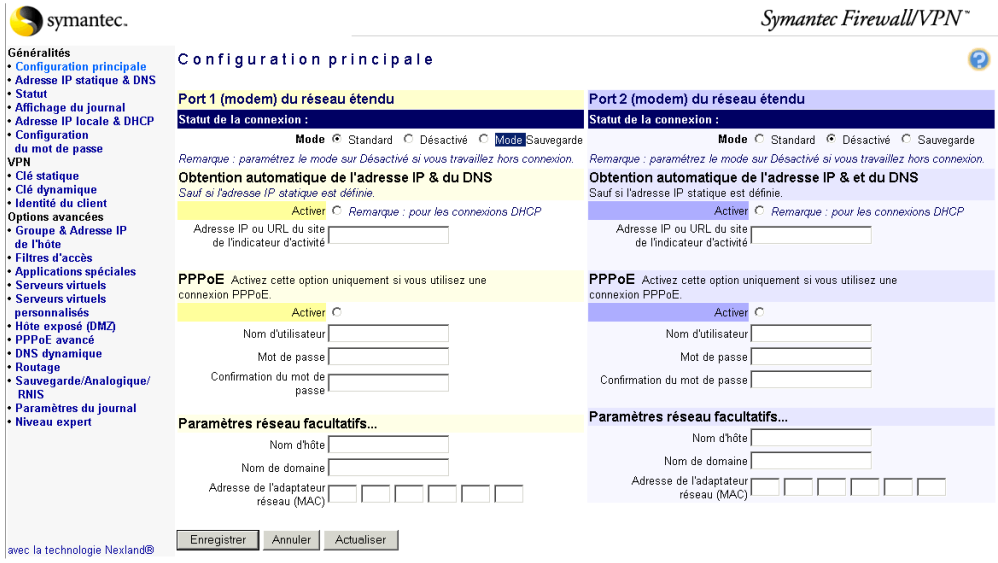



**Figure 3-1 : Ecran Configuration principale du Firewall/VPN200 Symantec**

L'écran **Configuration principale** est le premier écran que vous voyez quand vous allez sur le Firewall/VPN Symantec avec votre navigateur. Cet écran contient les paramètres de base indispensables pour pouvoir utiliser Internet. Cet écran sert à configurer les ports de réseau étendu 1 et 2.

La section **Statut de la connexion** en haut de l'écran indique si vous êtes : Connecté, en cours de connexion (pendant l'appel PPPoE) ou Déconnecté.

## Pour configurer le Firewall/VPN 200 Symantec avec l'écran Configuration principale

1. Si l'écran **Configuration principale** n'est pas affiché, cliquez sur **Configuration principale** dans le **Menu principal**. Le **Menu principal** est affiché en permanence sur le côté gauche de l'écran.

2. Effectuez l'une des opérations suivantes :

   - Si vous utilisez un compte d'accès à Internet dont l'adresse IP est fournie automatiquement par un serveur DHCP, cliquez sur le bouton radio **Activer** dans la section Obtention automatique de l'adresse IP & DNS.

     Ce bouton radio est activé par défaut et peut s'appliquer à la plupart des comptes d'accès par le câble. Cette option devrait vous permettre de vous connecter immédiatement (Statut de connexion Normal) si vous avez un compte de ce type. Si ce n'est pas le cas, cliquez sur le bouton **Réinitialiser** sur le Firewall/VPN.

     Si vous ne pouvez toujours pas vous connecter, vous devrez peut-être modifier l'adresse de l'adaptateur réseau (MAC). Pour plus d'informations, consultez la section « Section Paramètres réseau facultatifs » à la page 5.

     Si vous avez un compte Internet avec IP statique ou si vous utilisez le Firewall/VPN Symantec en interne ou sur un autre réseau, laissez ce paramètre sur Activé. Indiquez ensuite les informations d'IP statique sur l'écran IP statique & DNS, comme décrit dans la section « Adresse IP statique et DNS » à la page 8.

   - Si vous avez un compte Internet PPPoE, cliquez sur le bouton radio **Activer** dans la section **PPPoE**.

     Vous utilisez probablement PPPoE si vous utilisiez précédemment un logiciel de connexion à distance sur votre ordinateur avec un nom d'utilisateur et un mot de passe pour vous connecter avec un modem DSL. Le Firewall/VPN Symantec effectuera la connexion à distance automatiquement. Vous devez donc désactiver ou désinstaller le logiciel de connexion à distance).

     Vous devez aussi :

     a. Indiquer le nom d'utilisateur que votre FAI (fournisseur d'accès Internet) vous a fourni.

     b. Indiquer deux fois le mot de passe que votre FAI vous a fourni.

   Vous devriez être connecté en quelques instants. Vous pouvez avoir à redémarrer l'ordinateur pour actualiser les informations IP et pouvoir accéder à Internet. Si vous rencontrez des problèmes, vérifiez votre nom d'utilisateur et votre mot de passe PPPoE.

## Section Paramètres réseau facultatifs

Certains FAI ont besoin d'informations supplémentaires pour l'authentification. Si vous avez des problèmes pour vous connecter, vous pouvez saisir ces informations supplémentaires dans la section des informations facultatives de l'écran Configuration principale.

**Pour configurer les champs des paramètres réseau facultatifs**

1. Dans le champ Nom d'Hôte, indiquez le même nom d'hôte que celui de votre ordinateur.

   Vous devez saisir le nom d'hôte récupéré depuis l'ordinateur connecté au service Internet.

   **Remarque :** Les noms d'hôte et de domaine sont sensibles à la casse.

2. Dans le champ Nom de domaine, indiquez le même nom de domaine que celui de l'ordinateur qui était connecté à Internet. Les utilisateurs @Home doivent indiquer leur adresse électronique @Home complète pour pouvoir accéder au champ du nom de domaine de leur serveur de messagerie.

3. Indiquez votre adresse d'adaptateur réseau (MAC) dans les champs Adaptateur réseau (MAC).

   Certains FAI authentifient votre identité par rapport à l'adresse d'adaptateur (MAC) de votre carte Ethernet. Le Firewall/VPN Symantec peut avoir à simuler l'adresse de l'adaptateur de votre ordinateur pour pouvoir se connecter à votre FAI. Vous devez saisir l'adresse MAC récupérée sur l'ordinateur connecté au service Internet.

4. Cliquez sur **Enregistrer** après avoir fourni toutes les informations.

## Pour configurer un modem câble utilisant DHCP

Il est possible que vous soyez déjà connecté. Le statut de la connexion est indiqué en haut de l'écran Configuration principale. S'il indique "Connecté..." vous devriez pouvoir naviguer sur le Web.

Si vous avez un modem câble et que le statut de connexion indique Déconnecté...

1. Cliquez sur **Configuration principale**.

2. Allez dans la section **Paramètres réseau facultatifs** de cet écran.

3. Indiquez votre adresse d'adaptateur réseau (MAC) ou le nom d'hôte ou de domaine fourni par le FAI (fournisseur d'accès Internet).

4. Indiquez l'adresse MAC (voir ci-dessous) ou le nom d'hôte et de domaine dans les champs appropriés.

   **Remarque :** Les noms d'hôte et de domaine sont sensibles à la casse.

5. Cliquez sur **Enregistrer**. Le Firewall/VPN Symantec redémarre et essaye de se connecter à Internet.

6. Attendez quelques instants, puis cliquez sur la page **Revenir à la Configuration principale**.

7. Cliquez sur **Actualiser** dans le navigateur. Le Firewall/VPN Symantec doit indiquer **Connecté** dans le champ Statut de la connexion.

   Si ce n'est pas le cas, essayer d'actualiser de nouveau après quelques instants ou consultez le Chapitre 9 - Dépannage.

## Pour configurer DSL ou un modem câble avec PPPoE

Vous aurez besoin de votre nom d'utilisateur et de votre mot de passe pour continuer.

1. Cliquez sur **Configuration principale**.

2. Cliquez sur le bouton radio Activé sous l'en-tête PPPoE.

3. Dans le champ Nom d'utilisateur, indiquez votre nom d'utilisateur PPPoE exactement comme il vous a été indiqué par votre FAI (Fournisseur d'Accès Internet).

   **Remarque :** Certains FAI utilisent le nom de domaine dans le nom d'utilisateur pour l'ouverture de session (par exemple "john@gte.net"), alors que d'autres n'utilisent que l'ID de l'utilisateur (par exemple "john").

4. Dans le champ Mot de passe, saisissez votre mot de passe PPPoE.

5. Dans le champ Confirmation, saisissez de nouveau votre mot de passe PPPoE.

   Ce champ de confirmation permet de s'assurer qu'il n'y a pas de faute de frappe, car le mot de passe est masqué.

6. Cliquez sur **Enregistrer**.

7. Attendez quelques instants, puis cliquez sur **Revenir à la Configuration principale**.

8. Actualisez le navigateur.

   Vous devriez voir apparaître **Connecté** ou **Connexion en cours** dans le champ Statut de la connexion. Si ce n'est pas le cas, essayer d'actualiser de nouveau après quelques instants ou consultez le Chapitre 9 - Dépannage.

# Adresse IP statique et DNS

Si vous avez un compte avec IP statique chez votre FAI (fournisseur d'accès Internet) ou si vous utilisez le Firewall/VPN Symantec derrière une autre passerelle, fournissez les informations de réseau sur l'écran IP statique et DNS. Cet écran est similaire à l'écran des propriétés réseau d'un ordinateur.

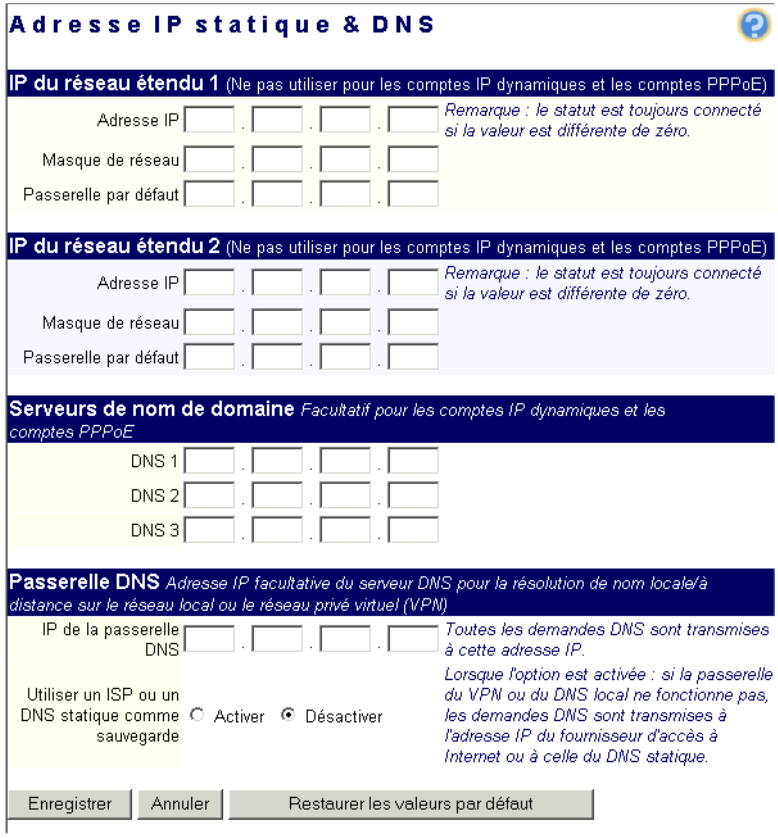



**Figure 3-2 : Ecran IP statique et DNS du Firewall/VPN 200 Symantec**

**Pour configurer l'écran IP statique et DNS**

Remplissez les informations de l'écran IP statique et DNS, comme suit :

1. Dans le champ Adresse IP de la section IP réseau étendu, saisissez l'adresse IP du côté extérieur (réseau étendu) du Firewall/VPN.

2. Dans le champ Masque réseau, saisissez le masque de réseau.

   Ce masque détermine où les paquets sont envoyés (en interne ou en externe). Certains comptes de FAI peuvent nécessiter une modification de ce paramètre ; sinon, laissez la valeur par défaut de 255.255.255.0 (réseau de classe "C").

3. Dans le champ Passerelle par défaut, indiquez la passerelle par défaut.

   Le Firewall/VPN Symantec envoie à la passerelle par défaut tous les paquets IP qu'elle ne sait pas acheminer.

4. Dans le champ Serveurs de noms de domaine, indiquez jusqu'à trois serveurs de noms de domaine.

   Ceux-ci sont nécessaires pour les comptes avec IP statique. Il n'est pas nécessaires de saisir des entrées pour les comptes Internet standard (IP dynamique) et les comptes dont les informations sont fournies par un serveur DHCP. Vous pouvez remplacer ces paramètres par les vôtres pour chaque compte Internet.

5. Cliquez sur **Enregistrer** après avoir fourni toutes les informations.

## Section Passerelle DNS

La Passerelle DNS est un serveur DNS optionnel  servant à la résolution de nom locale ou à distance sur les VPN. Toutes les demandes DNS sont transmises à l'adresse IP indiquée dans le champ de passerelle DNS. Si le serveur DNS interne ne fonctionne pas, l'unité peut être configurée pour faire suivre toutes les demandes DNS aux serveurs DNS du FAI (fournisseur d'accès Internet).

# Etat

L'écran d'Etat affiche les paramètres et la configuration actuels du Firewall/VPN.

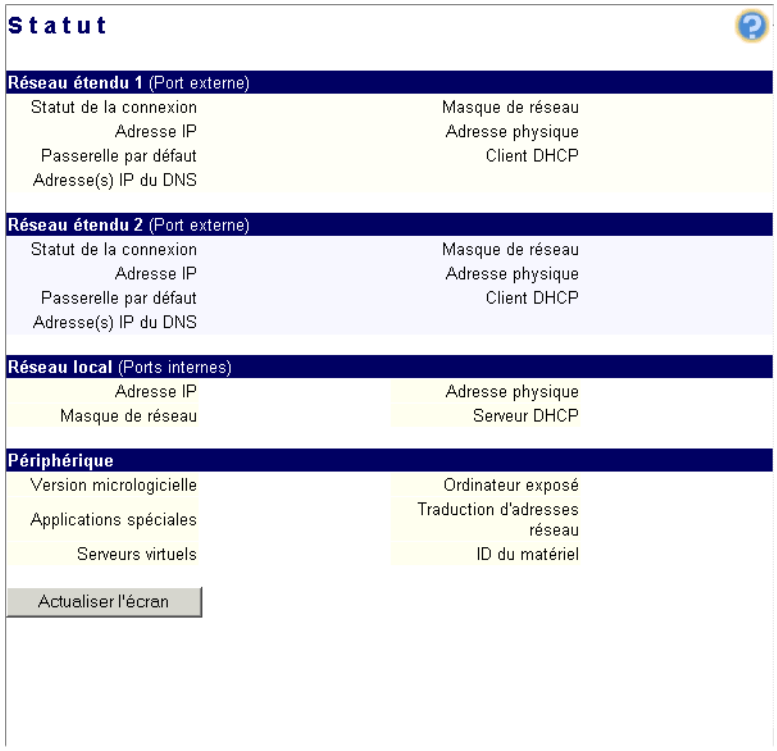



**Figure 3-3 : Ecran d'état**

L'adresse physique est l'adresse MAC du Firewall/VPN sur réseau local et étendu.

Si vous avez des problèmes pour accéder à Internet, vérifiez que vous avez une adresse IP de réseau étendu. Si c'est le cas, il peut y avoir un problème de DNS ou autre chez votre FAI. Dans tous les cas, ayez les informations de cet écran à portée de main quand vous appelez l'Assistance Symantec.

# IP de réseau local et DHCP

**Caution:** **NE CHANGEZ PAS ces paramètres sauf si cela est indispensable pour votre réseau. Vous risquez sinon de perdre la connectivité avec le Firewall/VPN, ce qui nécessiterait une réinitialisation manuelle aux valeurs par défaut.**

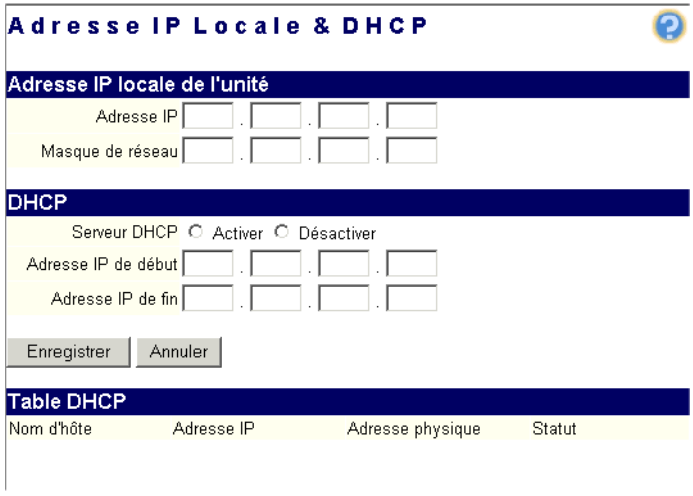



**Figure 3-4 : Ecran Adresse IP locale et DHCP**

## ADRESSE IP LOCALE DE L'UNITE

L'IP locale de l'unité est l'adresse IP du Firewall/VPN Symantec sur votre réseau local (vos hôtes la voient comme leur passerelle par défaut).

---

**Caution:** **Si vous modifiez l'adresse et que vous cliquez sur Enregistrer, VOUS NE POURREZ PLUS ACCEDER AU FIREWALL/VPN SYMANTEC SANS REDEMARRER (libérer et renouveler l'IP de votre hôte) parce que l'adresse IP, le masque de réseau et la passerelle auront changé.**

---

La combinaison de l'adresse IP et du masque de réseau détermine le sous-réseau de destination des paquets. Ces informations sont indispensables au routage correct des paquets sur un réseau IP. Certains comptes de FAI peuvent nécessiter une modification de ce paramètre ; si ce n'est pas le cas, laissez la valeur par défaut de 255.255.255.0 (réseau de classe "C").

## DHCP

Le Serveur DHCP du Firewall/VPN, activé par défaut, peut affecter des adresses IP et des informations DNS à un maximum de 253 ordinateurs connectés. Pour que cela fonctionne, vos ordinateurs doivent être configurés pour "Obtenir une adresse IP automatiquement" ou "Obtenir une adresse depuis un serveur DHCP" dans le Panneau de configuration (consultez la section « Configuration de l'ordinateur » à la page 7 pour plus d'informations).

Le Firewall/VPN Symantec affecte toujours une adresse IP au serveur DNS (192.168.0.1 par défaut) sauf si des DNS statiques sont définies. Cela est normal car le Firewall/VPN Symantec va gérer toutes les requêtes DNS envoyés au FAI (fournisseur d'accès Internet).

Vous pouvez désactiver le serveur DHCP dans le Firewall/VPN. Cela est utile si vous avez déjà un serveur DHCP sur votre réseau ou si tous les ordinateurs de votre réseau ont des adresses IP statiques définies dans leurs propriétés réseau. Par exemple, si vous avez un serveur Web sur votre site, vous devrez lui affecter une adresse statique.

La Plage DHCP représente la plage d'adresses IP que vous voulez que le serveur DHCP affecte.

La table DHCP liste tous les hôtes définis dans le serveur DHCP du Firewall/VPN, ainsi que leurs propriétés.

Si vous effectuez des changements, cliquez sur **Enregistrer** après avoir fourni toutes les informations.

# Mot de passe de configuration

Ce mot de passe protège l'interface Web du Firewall/VPN Symantec en demandant une authentification pour pouvoir accéder à l'unité. Nous vous recommandons de définir un mot de passe quand vous travaillez dans un environnement de bureau pour éviter toute reconfiguration incorrecte. Définissez toujours un mot de passe quand vous activez la configuration à distance (consultez le Niveau expert). De plus, pour des raisons de sécurité, Symantec recommande que toute gestion de l'unité à distance soit effectuée au travers d'un tunnel VPN.


**Figure 3-5 : Ecran Mot de passe de configuration**

**Remarque :** Le nom d'utilisateur est toujours admin pour se connecter au Firewall/VPN.

## Pour configurer un mot de passe

1. Saisissez le mot de passe.
2. Indiquez de nouveau le mot de passe pour le confirmer.
3. Cliquez sur **Enregistrer**.

Si vous oubliez votre mot de passe, vous devrez effectuer une réinitialisation manuelle (consultez le Chapitre 9 – Dépannage) ou réinitialiser l'unité par la console série. Le fait de reflasher le micrologiciel ne réinitialisera pas le mot de passe !

# Chapitre 4

# Configuration avancée

## PPPoE avancé

La plupart des utilisateurs n'ont pas besoin d'utiliser cette page car les paramètres par défaut du Firewall/VPN Symantec sont optimum pour la plupart des situations et permettent une totale transparence du fonctionnement des comptes PPPoE.

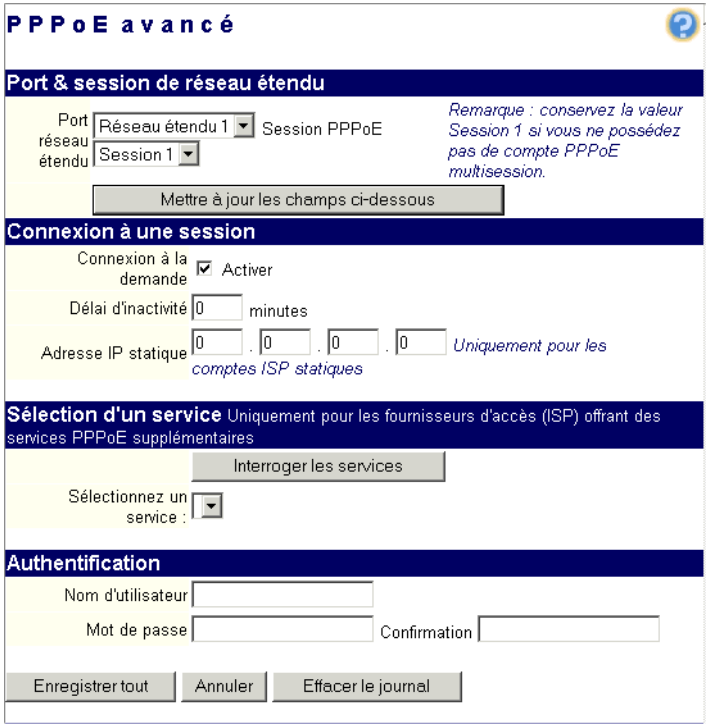



**Figure 4-1 : Ecran PPPoE avancé**

**Pour configurer l'écran PPPoE avancé**

**Remarque :** Vous devez être DECONNECTE pour utiliser cette fonctionnalité.

1. Sélectionnez le port de réseau étendu dans la liste déroulante **Port réseau étendu**.

2. Si vous avez un compte PPPoE multisession, sélectionnez la session appropriée dans la liste déroulante Session PPPoE.

   Répétez cette procédure pour chaque session PPPoE.

   Si vous avez un compte PPPoE mono session, laissez la valeur Session 1 pour le champ Session PPPoE.

3. Cliquez sur l'option **Mettre à jour les champs ci-dessous**.

4. Utilisez la section **Connexion à une session** pour spécifier si vous voulez connecter et déconnecter votre compte PPPoE manuellement ou automatiquement.

   a. L'option **Connexion à la demande** est activée par défaut ; le Firewall/VPN Symantec se connecte automatiquement quand une requête Internet est effectuée (comme la navigation sur un site Web). Si vous voulez vous connecter manuellement, désactivez cette case à cocher et connectez-vous en cliquant sur **Connecter**.

   b. Dans le champ **Délai d'inactivité**, indiquez la durée d'inactivité en minutes après laquelle le Firewall/VPN Symantec doit déconnecter la connexion PPPoE.

   c. Indiquez une valeur nulle pour que la connexion reste toujours active et empêcher le Firewall/VPN Symantec de raccrocher. Si la valeur indiquée est supérieure à 0, activez l'option **Connexion à la demande** pour vous reconnecter automatiquement quand c'est nécessaire.

   d. Si vous avez un compte Internet PPPoE avec IP statique, indiquez cette adresse IP dans le champ Adresse IP statique ; si ce n'est pas le cas, laissez ce champ sur la valeur 0.

   **Remarque :** Cela concerne uniquement PPPoE !

5. Si votre FAI (fournisseur d'accès Internet) propose différents services pour votre compte PPPoE, utilisez la section **Sélection d'un service** pour y accéder.

   a. Cliquez sur **Interroger les services.**

   b. Sélectionnez le service dans la liste déroulante puis connectez-vous normalement.

6. Indiquez votre **Nom d'utilisateur**.

7. Indiquez votre **Mot de passe**.

8. **Confirmez** votre mot de passe.

9. Cliquez sur **Enregistrer tout** pour traiter cet écran.

Le fichier journal de l'écran Affichage du journal fournit des informations utiles à propos de votre connexion PPPoE, si vous avez des problèmes à vous connecter à votre FAI.

# Service de DNS dynamique

Le Service de DNS dynamique est un système permettant aux gens de l'extérieur de se connecter à vos ordinateurs en utilisant un nom de domaine, même si vous avez un compte IP dynamique fourni par votre FAI (votre adresse IP change de temps en temps). Si vous mettez en place un Serveur Web virtuel, les gens pourront toujours y accéder en tapant votre nom de domaine ; par exemple www.mondnsdyn.com

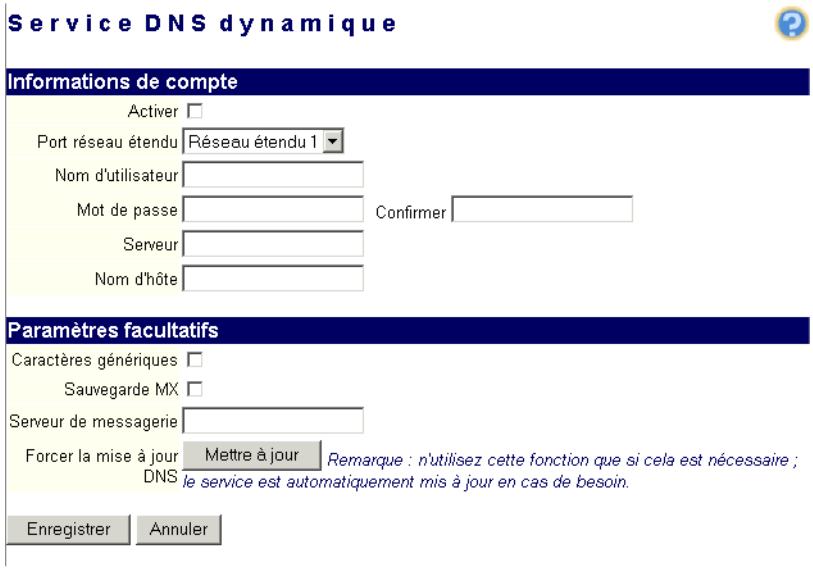



**Figure 4-2 : Ecran Service de DNS dynamique**

Le Firewall/VPN Symantec contacte un service DNS dynamique chaque fois que votre IP change et l'actualise automatiquement. Le service de DNS dynamique met ensuite à jour tous les serveurs DNS dans le monde entier. Les services DNS dynamiques existent en version payante et gratuite. Le client DNS dynamique intégré au Firewall/VPN Symantec est compatible avec la plupart des services standard.

**Pour configurer le DNS dynamique**

Les informations sur le client nécessaires pour remplir les champs ci-dessous peuvent être obtenues auprès de votre FAI.

1. Cliquez sur **Activer**.

2. Sélectionnez votre **Port réseau étendu** dans la liste déroulante **Port réseau étendu**.

3. Indiquez vos paramètres de bases.

   Ce sont les informations de votre compte. Indiquez ces informations exactement telles qu'elles vous sont fournies par le service.

4. Cliquez sur **Enregistrer.**

## Paramètres facultatifs de DNS dynamique

La configuration de ces paramètres n'est pas indispensable au fonctionnement, mais ils servent à faire suivre le courrier électronique en utilisant votre nouveau nom de domaine et nom secondaire. Le bouton de mise à jour forcée n'est là que pour les cas exceptionnels. Normalement, les services DNS dynamiques ne vous laissent pas mettre à jour manuellement vos informations sauf si votre IP change !

**Pour configurer les paramètres optionnels**

1. Cliquez sur **Caractères génériques**.

2. Cliquez sur **Sauvegarde MX**.

3. Entrez dans le **Serveur de messagerie**.

4. Cliquez sur **Enregistrer** après avoir fourni toutes les informations.

# Routage

S'il y a plusieurs routeurs sur un réseau, vous devez ajouter des paramètres de routage au Firewall/VPN, afin de lui indiquer quel trafic doit être envoyé vers chaque routeur. L'unité prend en charge les routes statiques ou le routage de protocole RIP2 (routage dynamique). Quand vous spécifiez le routage, le Firewall/VPN Symantec peut automatiquement retransmettre les paquets au routeur approprié.

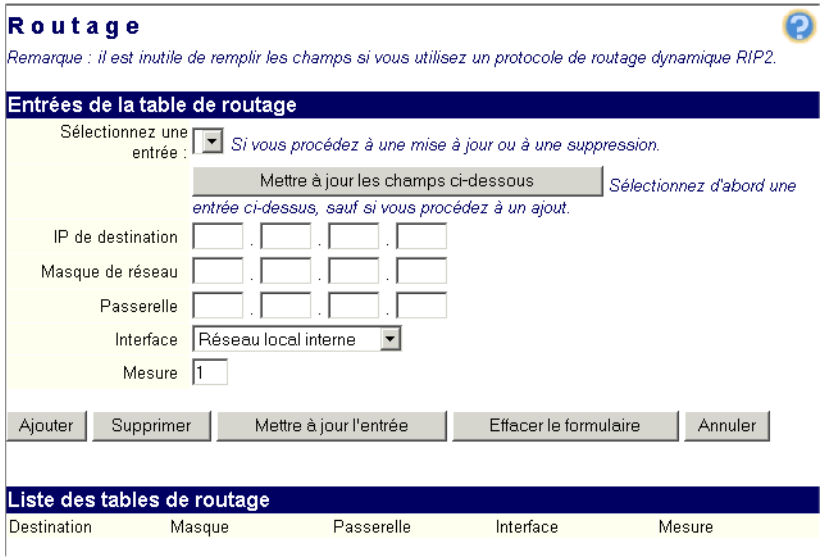



**Figure 4-3 : Ecran Routage**

Si RIP2 n'est pas en cours d'utilisation sur le réseau, vous devez ajouter des entrées à la table de routage statique au travers de l'écran Routage.

N'utilisez la table de routage statique que quand cela est nécessaire. Si vous définissez des entrées incorrectes, vous pouvez perdre la connexion à l'unité et avoir à effectuer une réinitialisation manuelle.

**Entrées existantes**

Si vous avez précédemment défini une entrée dans cet écran et que vous voulez la mettre à jour ou la supprimer, vous devez d'abord la sélectionner en utilisant **Sélectionner une entrée** puis cliquer sur **Mettre à jour les champs ci-dessous** pour accéder à ses paramètres. Si vous ajoutez une nouvelle entrée, cliquez sur **Effacer le formulaire** pour recommencer avec un formulaire vierge.

## Données de la table de routage

Une entrée dans la table de routage est requise pour chaque segment du réseau local afin que tous les autres segments connectés à ce périphérique puissent partager des données vers et depuis ce périphérique. Les données de la Table de routage sont les suivantes.

**Table 4-1 : Données de routage**

| | |
|---|---|
| IP de destination | Adresse réseau du segment de réseau distant. Pour les réseaux standard de classe "C", l'adresse réseau se compose des trois premiers champs de l'adresse IP de destination. Le quatrième champ (le dernier) peut avoir la valeur 0. |
| Masque de sous-réseau | Masque de sous-réseau utilisé sur le segment de réseau distant. Pour les réseaux de classe "C", le masque de sous-réseau est 255.255.255.0. |
| Passerelle | Adresse IP du routeur sur le segment de réseau auquel ce périphérique est connecté, PAS celle du routeur sur le segment de réseau distant. Normalement désigné saut suivant sur le réseau. |
| Interface | Sélectionnez l'interface appropriée dans les réseaux locaux et étendus. Les utilisateurs du modèle 200 peuvent choisir parmi deux interfaces. |
| Mesure | Nombre de routeurs qu'il faut traverser pour atteindre le segment de réseau local distant. La valeur par défaut est 1. |

## Les autres routeurs du réseau local

Les autres routeurs du réseau local doivent utiliser le routeur local de Firewall/VPN Symantec comme routeur local par défaut. Les entrées seront les mêmes que pour le routeur local du Firewall/VPN Symantec, sauf pour l'adresse IP de passerelle.

Pour un routeur avec connexion directe au routeur local du Firewall/VPN Symantec, l'adresse IP de passerelle est l'adresse du routeur local du Firewall/VPN Symantec.

Pour les routeurs qui doivent faire suivre les paquets à un autre routeur avant d'atteindre le routeur local du Firewall/VPN Symantec, l'adresse IP de passerelle est l'adresse du routeur intermédiaire.

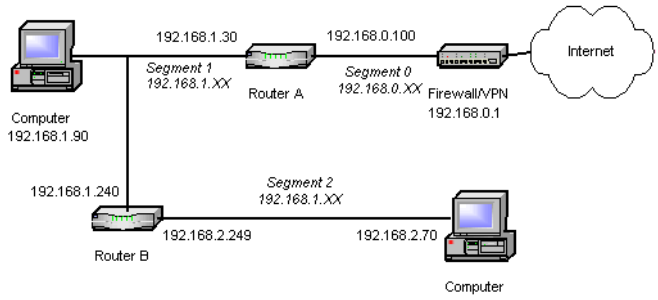



**Figure 4-4 : Exemple de routage**

Pour le réseau local illustré ci-dessus, avec deux routeurs et trois segments de réseau, la table de routage du Firewall/VPN nécessite deux entrées :

**Entrée 1 (Segment 1)**

Adresse IP de destination 192.168.1.0
Masque de sous-réseau 255.255.255.0
Adresse IP de passerelle 192.168.10.100
Métrique 1

**Entrée 2 (Segment 2)**

Adresse IP de destination 192.168.1.0
Masque de sous-réseau 255.255.255.0
Adresse IP de passerelle 192.168.10.100
Métrique 2

**Pour la route par défaut du routeur A**

Adresse IP de destination 0.0.0.0
Masque de sous-réseau 0.0.0.0
Adresse IP de passerelle 192.168.0.1 (adresse IP du Firewall/VPN Symantec)

**Pour la route par défaut du routeur B**

Adresse IP de destination 0.0.0.0
Masque de sous-réseau 0.0.0.0
Adresse IP de passerelle 192.168.1.30 (routeur local du Firewall/VPN Symantec)

# Groupe et Adresse IP de l'hôte

Cet écran vous permet d'affecter des IP statiques, de définir le groupe d'accès (voir Filtres d'accès) et de lier des sessions PPPoE multiples à des hôtes individuels sur le réseau local. Les IP statiques (réservations dans la table DHCP du Firewall/VPN Symantec) doivent être affectées pour tous les serveurs virtuels, tous les ordinateurs portables (pour éviter les conflits IP pendant que leurs cartes sont en veille) et toutes les imprimantes connectés directement au réseau local.

Avec le Firewall/VPN modèle 200, vous pouvez associer un hôte à un port de réseau étendu spécifique. Cela empêche l'hôte d'utiliser les deux ports de réseau étendu en cas de liaison de connexion large bande. Cette fonction est utile pour les serveurs et les applications qui doivent toujours être situés à une IP spécifique. Le paramètre par défaut est Désactiver.

**Sélectionnez un hôte :** Si vous avez précédemment défini une entrée dans cet écran et que vous voulez mettre à jour ou supprimer cette entrée, vous devez d'abord la sélectionner dans la liste déroulante puis cliquer sur **Mettre à jour les champs ci-dessous** pour accéder à ses paramètres. En revanche, si vous ajoutez une nouvelle entrée, n'en sélectionnez pas dans la liste déroulante ou cliquez sur **Effacer le formulaire** avant d'ajouter la nouvelle entrée.


**Figure 4-5 : Groupe et adresse IP de l'hôte**

### Pour configurer le groupe et l'adresse IP de l'hôte

1. Dans la section Identité du réseau hôte, indiquez un nom d'hôte.

   Donnez à l'hôte un nom court et explicite. Ce nom peut être le même que celui défini dans les propriétés réseau de l'ordinateur, mais ce n'est pas obligatoire.
2. Indiquez l'adresse de l'adaptateur réseau.

   Le Firewall/VPN Symantec identifie l'hôte par l'adresse d'adaptateur de sa carte d'interface réseau (généralement une carte Ethernet). Vous devez indiquer l'adresse de la carte d'interface réseau de l'hôte dans ce champ.

3. Dans la section Paramètres de l'hôte, cochez l'option **Réserver l'entrée dans la table DHCP** pour affecter une IP locale statique à l'ordinateur par l'intermédiaire du serveur DHCP du Firewall/VPN.

   Cela signifie que le Firewall/VPN Symantec réservera automatiquement l'adresse IP correspondante pour cet hôte spécifique et n'accordera cette IP qu'à cet hôte, quel que soit le moment auquel il démarre. Vous pouvez laisser les propriétés réseau de l'ordinateur sur l'option **Obtenir l'adresse IP automatiquement** car le Firewall/VPN Symantec veillera à ce que l'IP reste la même.

4. Dans le champ Adresse IP réservée, indiquez l'adresse IP que vous voulez affecter à cet ordinateur.

   Elle doit se trouver sur la même classe de réseau que le Firewall/VPN Symantec. S'il s'agit d'un serveur virtuel, vérifiez que l'adresse IP correspond à celle indiquée sur l'écran Serveur virtuel. (Consultez la section « Serveurs virtuels » à la page 16).

5. Sélectionnez le groupe de cet hôte dans la liste déroulante Groupe d'accès.

   Les groupes d'accès sont définis sur l'écran Filtres d'accès.

6. Dans la liste déroulante Liaison à la session PPPoE, sélectionnez la session à lier à cet hôte.

   N'utilisez cette procédure que si de multiples sessions PPPoE sont définies. Elle nécessite un compte PPPoE spécial auprès de votre FAI (fournisseur d'accès Internet).

7. Cliquez sur **Ajouter** pour ajouter la nouvelle entrée ou :

   Cliquez sur **Supprimer** pour supprimer l'entrée affichée et libérer la mémoire du Firewall/VPN Symantec.

   Cliquez sur **Mettre à jour l'entrée** si vous avez modifié l'entrée affichée.

   Cliquez sur **Effacer le formulaire** avant d'ajouter une nouvelle entrée.

# Filtres d'accès

Les filtres d'accès permettent de contrôler les types d'informations autorisés à sortir de votre réseau local. Par exemple, pour autoriser l'utilisation de Real Audio sur le réseau local, vous pouvez sélectionner ce protocole ici ou sélectionner l'option **Aucune restriction**. La plupart des protocoles standard sont prédéfinis mais vous pouvez définir des filtres personnalisés. Vous pouvez définir cinq groupes de sécurité pour spécifier différents niveaux d'accès pour les différents ordinateurs.

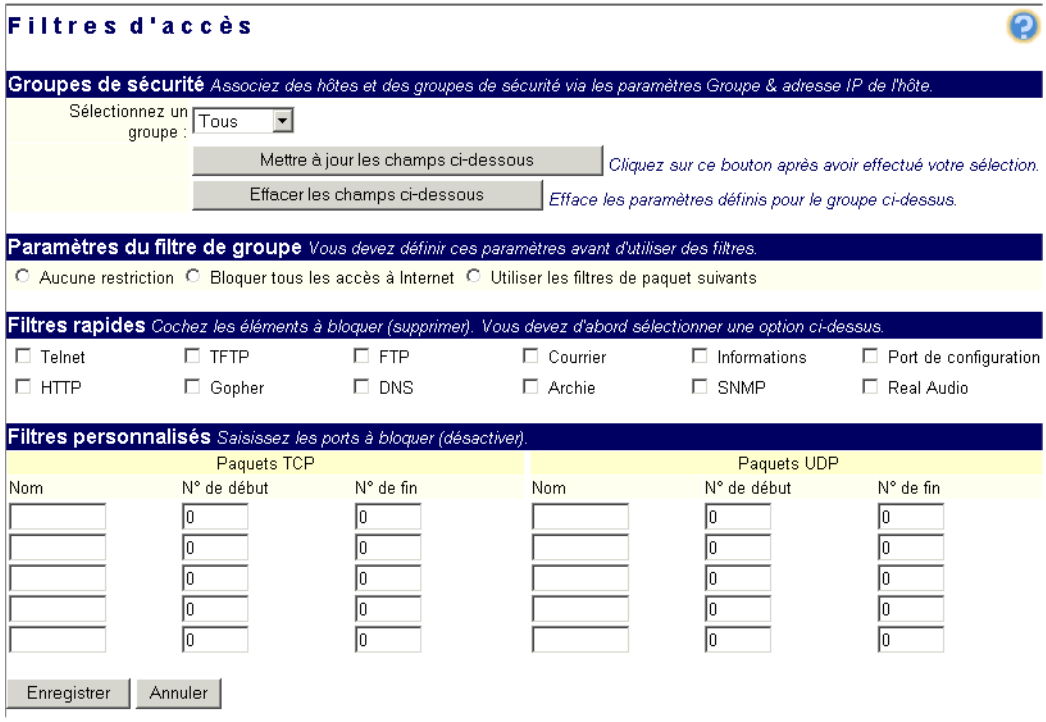



**Figure 4-6 : Filtres d'accès**

## Groupes de sécurité

Par défaut, tous les ordinateurs font partie du groupe Tous et ne sont soumis à aucune restriction sur l'utilisation d'Internet. Si vous voulez définir des filtres, commencez par

sélectionner le groupe, spécifiez l'utilisation des filtres de paquets puis indiquez les filtres à utiliser pour ce groupe sur cet écran.

Pour modifier une entrée précédemment définie, sélectionnez-la dans la liste déroulante puis cliquez sur **Mettre à jour les champs ci-dessous** pour accéder à ses paramètres.

**Remarque :** Vous devez LIER les hôtes locaux au groupe dont ils font partie dans l'écran Groupe & adresse IP de l'hôte, comme expliqué dans la section « Groupe et Adresse IP de l'hôte » à la page 9.

**Pour configurer les filtres d'accès**

**Remarque :** Cliquez toujours sur **Enregistrer** après avoir défini chaque paramètre de groupe

1. Sélectionnez votre Groupe de sécurité dans la liste déroulante **Sélectionnez un groupe**.

   Associez les hôtes à des groupes de sécurité en utilisant l'écran Groupe & adresse IP.

2. Cliquez sur **Mettre à jour les champs ci-dessous**.

3. Dans la section Paramètres du filtre de groupe, cliquez sur le bouton radio **Utiliser les filtres de paquet suivants**.

   Cette section définit le paramètre global s'appliquant au groupe sélectionné. Vous DEVEZ choisir **Utiliser les filtres de paquet suivants** pour sélectionner les filtres.

4. Dans la section **Filtres rapides**, cochez les éléments que vous voulez bloquer.

5. Dans la section **Filtres personnalisés**, indiquez un nom court et les ports de début et de fin utilisés par le protocole.

   Vous devez connaître le type de paquet (TCP ou UDP) et les ports utilisés par le protocole que vous voulez bloquer. Si un seul port est utilisé, indiquez le même numéro dans les deux champs. Vous pouvez définir des protocoles et des plages multiples pour obtenir des filtres très souples pour chaque groupe.

6. Cliquez sur **Enregistrer** après avoir indiqué toutes les informations pour un groupe.

# Applications spéciales

Certaines applications utilisant des communications bidirectionnelles ont besoin que des ports soient ouverts dans le firewall pour fonctionner. C'est le cas de la plupart des jeux et des logiciels de vidéo/téléconférence. Certains logiciels connus sont déjà prédéfinis mais désactivés par défaut. Vous pouvez les activer ici ou ajouter de nouvelles entrées. Pour déterminer les ports et les protocoles dont votre application a besoin pour fonctionner, il est préférable de consulter l'aide de cette application et de rechercher les paramètres associés à l'utilisation d'un Firewall ou du NAT. Certaines applications peuvent nécessiter l'ajout et l'activation de plusieurs entrées, par exemple quand une application utilise plusieurs plages de ports.

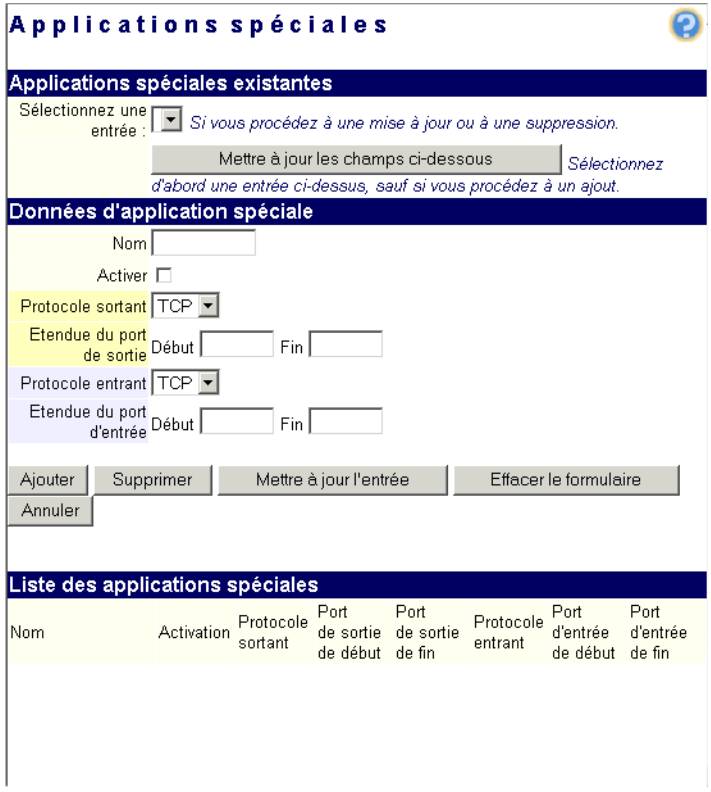



**Figure 4-7 : Ecran Applications spéciales**

**Pour configurer les applications spéciales**

1. Dans la section **Applications spéciales**, sélectionnez une entrée dans la liste déroulante.

   Certaines entrées prédéfinies pour les applications spéciales sont accessibles dans ce menu (comme elles sont toutes désactivées par défaut, vous devez sélectionner, activer et mettre à jour l'entrée), conjointement à toutes les entrées que vous avez définies vous-même.

   Si vous avez précédemment défini une entrée dans cet écran et que vous voulez Mettre à jour ou Supprimer cette entrée, vous devez d'abord la sélectionner dans la liste déroulante puis cliquer sur **Mettre à jour les champs ci-dessous** pour accéder à ses paramètres. Cela est valable pour l'activation des Applications spéciales prédéfinies.

   Si vous ajoutez une nouvelle entrée, n'en sélectionnez pas dans la liste déroulante ou cliquez sur **Effacer le formulaire** avant d'ajouter la nouvelle entrée.

2. Dans le champ **Données d'application spéciale**, saisissez le nom de cette application spéciale dans le champ Nom.

   Donnez un nom court et explicite à cette application spéciale.

3. Sélectionnez ou désélectionnez l'option **Activer** pour activer ou désactiver l'application spéciale (la désactivation ferme les ports définis).

   Pensez à cliquer sur **Mettre à jour** si vous utilisez une application spéciale existante.

4. Dans la liste déroulante Protocole sortant, choisissez TCP ou UDP comme type de protocole pour envoyer les données (consultez l'assistance de l'application).

5. Dans les champs Etendue du port de sortie, indiquez les ports de début et de fin utilisés par votre application pour envoyer des données. Si un seul port est utilisé, indiquez le même numéro dans les deux champs.

6. Dans le champ Protocole entrant, choisissez TCP ou UDP comme type de protocole pour recevoir des données (consultez l'assistance de l'application).

7. Dans les champs Etendue du port d'entrée, indiquez les ports de début et de fin utilisés par votre application pour recevoir des données.

   Si un seul port est utilisé, indiquez le même numéro dans les deux champs.

8. Cliquez sur **Ajouter** pour ajouter une nouvelle entrée.

   Cliquez sur **Supprimer** pour supprimer l'entrée affichée et libérer la mémoire du Firewall/VPN Symantec.

   Cliquez sur **Mettre à jour l'entrée** si vous avez modifié l'entrée affichée.

   Cliquez sur **Effacer le formulaire** avant d'ajouter une nouvelle entrée.

# Serveurs virtuels

Les serveurs virtuels vous permettent d'héberger tout type de serveur standard (Web, FTP, DNS, WhoIs, POP3, Finger, SMTP, VPN, News, Gopher, et Telnet) en utilisant le Firewall/VPN Symantec. Cela vous permet de mettre en place un serveur Web derrière le firewall. Les utilisateurs externes se connectent à un domaine affecté par la fonctionnalité de DNS dynamique ou à l'adresse IP du port modem pour accéder à un serveur virtuel. Le Firewall/VPN Symantec achemine automatiquement le trafic vers l'IP d'hôte appropriée sur le réseau local.

## Types de serveurs virtuels

Le Firewall/VPN Symantec accepte deux types de serveurs virtuels :

- Prédéfinis - Types de serveurs standard. Le seul paramètre nécessaire est l'adresse IP du serveur sur votre réseau local.
- Personnalisés - Serveurs non standard. Vous devez fournir des informations supplémentaires sur le serveur (numéros de ports TCP ou UDP). Vous utilisez pour cela l'écran Serveur virtuel personnalisé.

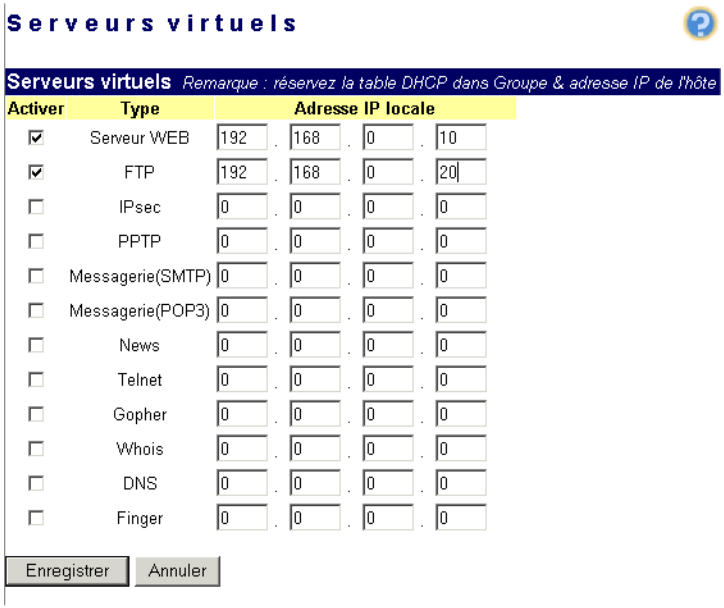



**Figure 4-8 : Ecran Serveurs virtuels**

## Pour configurer un serveur virtuel

1. Affectez une adresse IP locale statique à votre serveur dans l'écran Groupe & adresse IP (ou sur le serveur lui-même).

   Pour fonctionner efficacement, les serveurs virtuels nécessitent un hôte local avec une adresse IP statique.

2. Cochez l'option **Activer** à côté du type du serveur.

   Indiquez l'adresse IP de l'hôte sur le réseau local pour activer un serveur virtuel prédéfini. Vous pouvez avoir différents serveurs virtuels dirigés vers le même hôte.

3. Cliquez sur **Enregistrer**.

## Exemple de serveurs virtuels - adresse IP vue par les utilisateurs d'Internet

Le diagramme suivant (*Figure 4-9, à la page 4-18* ) représente un réseau où les utilisateurs d'Internet se connectent à la même adresse IP, mais utilisent des protocoles et/ou des numéros de ports différents. Pour les utilisateurs d'Internet, tous les serveurs virtuels de votre réseau ont la même adresse IP. Il s'agit de l'adresse IP définie dans le champ Port réseau étendu affiché dans l'écran STATUT. L'écran précédent Serveurs virtuels ( *Figure 4-8 à la page 4-17*) affiche la configuration pour cet exemple.

La fonction **Hôte exposé** ou **DMZ** est disponible pour un seul ordinateur du réseau local. Cette fonction expose à l'extérieur tous les ports de l'hôte spécifié. Pour des raisons de sécurité, cette fonction doit être désactivée quand vous n'en avez pas besoin. Si vous avez des problèmes avec une application qui utilise Internet, vous pouvez utiliser cette fonctionnalité pour effectuer un dépannage. Il peut être utile de créer une application spéciale (consultez la section « Applications spéciales » à la page 14 ) ou un serveur virtuel (consultez la section « Serveur virtuel personnalisé » à la page 19). Vous devez choisir un port de réseau étendu pour exposer l'hôte.

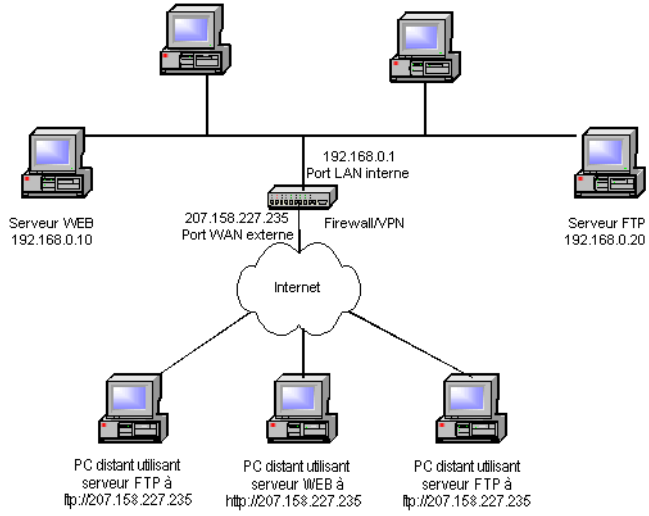



**Figure 4-9 : Exemple de réseau avec serveur virtuel**

# Serveur virtuel personnalisé

Cette fonction permet de définir un serveur personnalisé accessible depuis l'extérieur par l'adresse IP de réseau étendu externe du Firewall/VPN. Le Firewall/VPN Symantec redirige alors la requête vers l'adresse IP locale interne du serveur virtuel. Vérifiez d'abord sur l'écran **Serveurs virtuels** que votre serveur n'est pas déjà prédéfini.

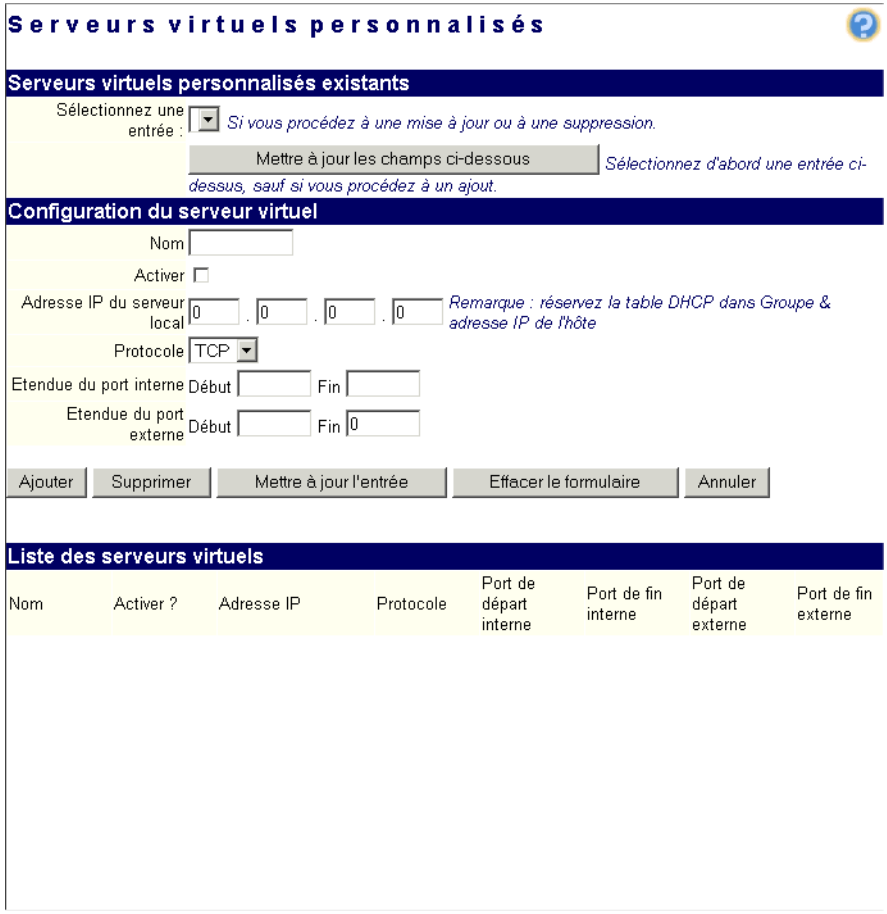



**Figure 4-10 : Ecran Serveurs virtuels personnalisés**

## Serveurs virtuels personnalisés existants

Si vous avez précédemment défini une entrée dans cet écran et que vous voulez mettre à jour ou supprimer cette entrée, vous devez d'abord la sélectionner dans la liste déroulante **Sélectionnez une entrée** puis cliquer sur **Mettre à jour les champs ci-dessous** pour accéder à ses paramètres. Si vous ajoutez une nouvelle entrée, n'en sélectionnez pas dans la liste déroulante ou cliquez sur **Effacer le formulaire** avant d'ajouter la nouvelle entrée.

**Pour configurer un serveur virtuel personnalisé**

1. Dans la section Configuration du serveur virtuel, dans le champ Nom, saisissez un nom décrivant votre serveur virtuel personnalisé.

2. Sélectionnez ou désélectionnez l'option **Activer** pour activer ou désactiver votre serveur.

   Veillez à cliquer sur **Mettre à jour l'entrée** si vous utilisez un Serveur virtuel existant.

3. Indiquez l'adresse IP de votre serveur sur le réseau local.

   Pour fonctionner efficacement, les serveurs virtuels nécessitent un hôte local avec une adresse IP statique. Affectez une adresse IP locale statique à votre serveur dans l'écran Groupe & adresse IP (ou sur le serveur lui-même). Indiquez cette IP ici.

4. Choisissez TCP ou UDP comme type de protocole pour le serveur.

5. Dans les champs des plages de ports, indiquez les ports de début et de fin utilisés par votre serveur en Interne et en Externe.

   Si un seul port est utilisé, indiquez le même numéro dans les deux champs Début et Fin. En général, les valeurs pour Interne et Externe seront identiques mais vous pouvez effectuer une translation sur les ports en indiquant des valeurs différentes (par exemple 2000-2500 en interne peut devenir 3000-3500 en externe par translation).

6. Cliquez sur **Ajouter** pour ajouter une nouvelle entrée ou effectuez l'une des opérations suivantes :

Cliquez sur **Supprimer** pour supprimer l'entrée affichée et libérer la mémoire du Firewall/VPN Symantec.

Cliquez sur **Mettre à jour** si vous avez modifié l'entrée affichée.

Cliquez sur **Effacer le formulaire** avant d'ajouter une nouvelle entrée.

# Hôte exposé (DMZ)

Cet écran vous permet de définir un serveur personnalisé accessible depuis l'extérieur par l'adresse IP de réseau étendu externe du Firewall/VPN Symantec. L'unité redirige vers l'hôte exposé toutes les requêtes qui ne sont pas explicitement autorisés par une règle de serveur virtuel. Le Firewall/VPN Symantec redirige ensuite la requête vers l'adresse IP locale interne du serveur virtuel. Vérifiez d'abord sur l'écran Serveurs virtuels que votre serveur n'est pas déjà prédéfini. Pour des raisons de sécurité, veillez à ce que la machine exposée soit "verrouillée" afin d'éviter tout accès non autorisé qui mettrait en danger la sécurité du système.

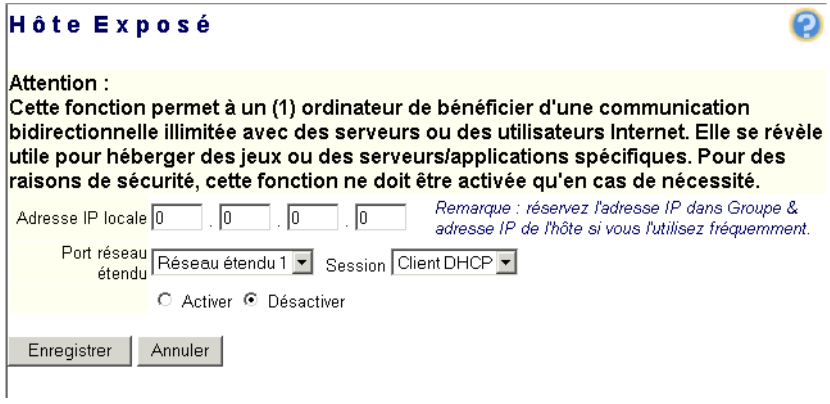



**Figure 4-11 : Hôte exposé (DMZ)**

**Pour configurer un hôte exposé**

1. Indiquez l'adresse IP locale de l'hôte que vous voulez exposer.
2. Sélectionnez le port de réseau étendu dans la liste déroulante Port réseau étendu.
3. Sélectionnez la session dans la liste déroulante Session.
4. Sélectionnez l'option **Activer**.
5. Cliquez sur **Enregistrer**.

## Niveau expert

Cet écran contient les paramètres avancés du Firewall/VPN Symantec. La plupart des utilisateurs peuvent ignorer ces paramètres sans problème car les valeurs par défaut sont optimales et les plus sûres.

Le Firewall/VPN 200 Symantec offre une connexion large bande par liaison de ses deux ports modem. Vous pouvez mélanger les types de connexion sur les deux ports (recommandé pour des raisons de sauvegarde). Vous pouvez par exemple agréger une connexion Internet par câble et une connexion DSL ou une IP statique et SDSL, PPPoE et DHCP.

Le Firewall/VPN 200 Symantec peut agréger la bande passante de vos deux connexions en envoyant des paquets réseau sur les deux ports de réseau étendu. Si vous le souhaitez, vous pouvez associer des hôtes à un même port de réseau étendu. Aucun téléchargement du réseau ne pourra dépasser la bande passante maximale disponible sur un seul port de réseau étendu mais cela permettra d'améliorer grandement les performances sur tout le réseau. Plus le nombre d'ordinateurs est élevé, plus les performances augmenteront sur une seule connexion Internet.

Si vous effectuez des modifications dans l'écran Niveau expert, cliquez sur **Enregistrer**.

Si vous cliquez sur **Restaurer les valeurs par défaut**, le Firewall/VPN Symantec revient à ses paramètres d'usine.

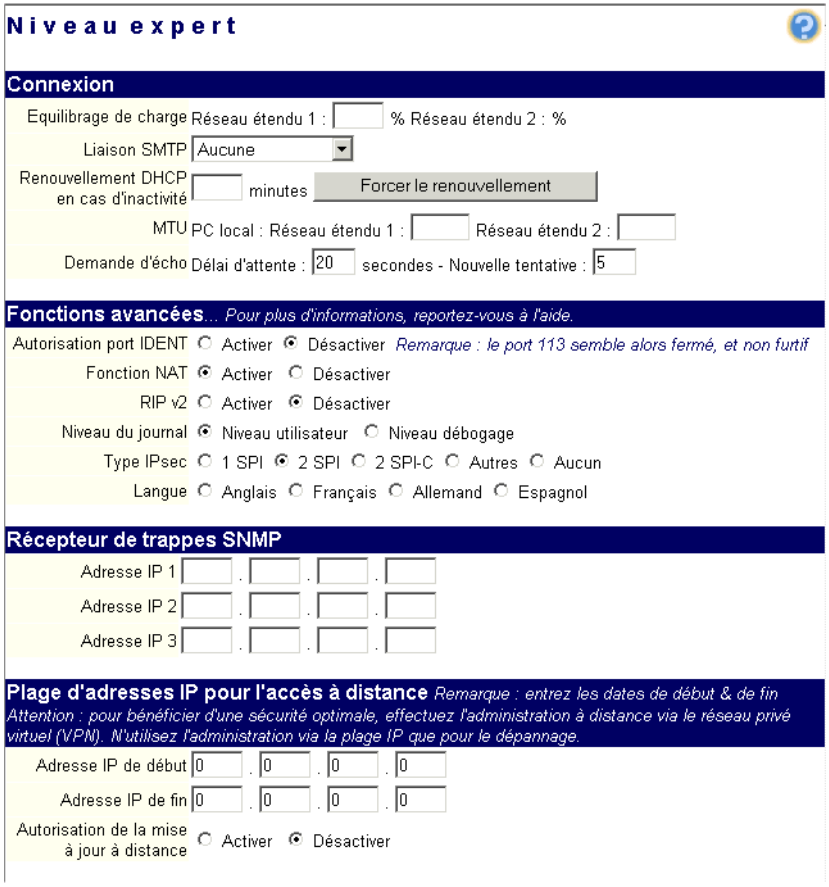



**Figure 4-12 : Ecran Niveau expert**

# Champs Connexion du Niveau expert

## Equilibrage de charge

Vous pouvez définir manuellement sur le Firewall/VPN 200 ou 200R Symantec l'équilibrage de charge à utiliser quand la liaison de connexion large bande est utilisée. Ce paramètre détermine le pourcentage de paquets envoyés à chaque port réseau étendu. Avec les connexions lentes, utilisez une valeur inférieure pour ce port de réseau étendu pour obtenir des performances optimales. Vous n'avez besoin d'indiquer que le pourcentage du port de réseau étendu n°1, le pourcentage du port de réseau étendu n°2 est déduit.

## Liaison SMTP

Si vous avez des comptes Internet de FAI (fournisseur d'accès Internet) différents connectés simultanément, vous devez vous assurer que votre courrier électronique (protocole SMTP) n'est transmis que sur la connexion réseau étendu associée à votre serveur de courrier électronique. Sinon, le serveur peut rejeter le courrier envoyé depuis un autre domaine. Vous pouvez choisir Réseau étendu 1 ou Réseau étendu 2. "Aucuen" (liaison) est la valeur par défaut.

## Renouvellement DHCP en cas d'inactivité

Si vous avez des problèmes de déconnexion avec un compte Internet de type DHCP après un certain délai d'inactivité, indiquez dans ce champ la durée (en minutes) après laquelle le Firewall/VPN Symantec doit essayer automatiquement de renouveler la connexion. Faites des essais pour déterminer la meilleure valeur, qui sera la plus élevée possible. Vous pouvez aussi forcer le renouvellement en cliquant sur le bouton correspondant.

## MTU PC réseau local

Le Firewall/VPN Symantec négocie la taille de la MTU avec votre FAI. Laissez cette valeur telle quelle sauf si le FAI fournit une taille de MTU qui n'est pas optimale. Les problèmes de MTU se traduisent par des difficultés pour consulter certains sites Web ou envoyer de longs messages électroniques, ou par des performances extrêmement dégradées. Vous pouvez définir la taille de MTU pour chaque port réseau étendu.

## Délai de demande d'écho

Ne changez pas ce paramètre, sauf spécification contraire de l'Assistance Symantec.

# Niveau expert - Champs de la section Fonctions avancées

## Autorisation port IDENT

Le port 113 (IDENT) contient normalement les informations de Nom d'hôte et de Nom de société. Par défaut tous les ports du Firewall/VPN Symantec sont en mode furtif. Cela rend vos ordinateurs invisibles depuis l'extérieur. Certains serveurs (comme des serveurs de messagerie ou MIRC) utilisent le port IDENT du système lors des accès. L'activation de ce paramètre rend le Port 113 "fermé", et non "furtif" (il n'est PAS ouvert). Ne l'activez que si vous avez des problèmes pour accéder à un serveur.

## Fonction NAT

La désactivation de la fonction NAT transforme le Firewall/VPN Symantec en pont ou routeur pur. Cela est utile si vous avez déjà un périphérique NAT sur votre réseau et que vous souhaitez utiliser le Firewall/VPN Symantec uniquement en tant périphérique de "connexion à distance" PPPoE. Des entrées doivent être présentes dans la table de routage ou vous devez utiliser RIP2 pour des communications correctes avec NAT désactivé.

## RIP V2

Vous permet d'activer la fonctionnalité RIP2 de l'unité. RIP2 est un protocole de routage dynamique utilisé pour diriger le trafic sur les réseaux avec routage.

## Niveau du journal

En choisissant l'option Niveau débogage, vous consignez des informations plus détaillées dans le journal d'état, ce qui peut être utile à l'Assistance Symantec. Cela envoie également tous les paquets périphériques de réseau étendu dans le réseau local pour faciliter l'analyse des ports. Laissez ce paramètre sur Niveau utilisateur sauf si vous avez besoin du mode Débogage, car celui-ci peut provoquer des collisions en cas de charge de trafic élevée.

## Type IPsec

La fonction de transmission directe IPsec est implémentée automatiquement par le Firewall/VPN Symantec. Laissez cette option sur 2 SPI sauf spécification de l'Assistance Symantec. L'option Aucun vous permet d'utiliser votre client VPN dans le mode Hôte exposé (DMZ) si vous avez des problèmes de connexion depuis derrière le Firewall/VPN Symantec.

## Langue

Vous pouvez choisir l'une des langues disponibles pour l'interface utilisateur en cochant la case située à côté de la langue.

## Niveau expert - Champs de la section Récepteur de trappes SNMP

Définit les IP devant recevoir les alertes de trappe émises par l'unité.

## Niveau expert - Champs de la section Plage d'adresses IP pour l'accès à distance

L'interface Web du Firewall/VPN Symantec est accessible à distance depuis une plage d'adresses IP. Pour des raisons de sécurité, Symantec recommande que toute la gestion externe à distance soit effectuée par l'intermédiaire d'un tunnel VPN. En utilisant un tunnel VPN, il vous suffit d'aller à l'adresse IP interne du Firewall/VPN Symantec avec votre navigateur.

Pour configurer l'unité à distance, indiquez le début et la fin de la plage IP (indiquez la même valeur pour les deux si vous voulez définir une seule adresse IP). Vous pouvez ensuite accéder à l'unité depuis un navigateur Web externe en tapant l'IP du port réseau étendu suivi du port 8088.

Par exemple : saisissez "http://207.158.227.235:8088" dans votre navigateur externe, si 207.158.227.235 est l'adresse obtenue auprès de votre FAI par le Firewall/VPN Symantec. L'IP depuis laquelle vous vous connectez doit être incluse dans la plage IP spécifiée. Vous avez aussi intérêt à spécifier un mot de passe de configuration pour plus de sécurité.

## Autorisation de la mise à jour à distance

Vous pouvez activer l'option **Autorisation de la mise à jour à distance** si vous souhaitez effectuer des mises à niveaux TFTP à distance du micrologiciel de l'unité depuis la plage IP spécifiée au-dessus. La valeur par défaut est **Désactivé**.

# Chapitre 5

# Configuration de réseaux privés virtuels (VPN - Virtual Private Networks)

Ce chapitre décrit les procédures de configuration de tunnels VPN avec les fonctionnalités VPN – Clé statique, VPN – Clé dynamique et VPN – Identité du client de l'interface utilisateur de Symantec Firewall/VPN. Il contient également une brève présentation des VPN, du cryptage et de l'authentification.

Les VPN permettent aux entreprises d'utiliser en toute sécurité des canaux de communication non sécurisés pour transporter des données sensibles. La technologie VPN la plus répandue dans l'industrie est basée sur les standards IPSec (IP Security – Sécurité IP). IPSec est un ensemble de standards approuvés par l'IETF (Internet Engineering Task Force – groupe de travail de développement d'Internet). La suite IPSec comporte des protocoles de sécurité permettant de garantir l'intégrité et la confidentialité des données grâce au cryptage. L'intégrité des données interdit que les données soient modifiées pendant les transferts. Elle garantit que les données reçues par le destinataire sont exactement celles qui ont été envoyées par l'expéditeur. La confidentialité des données garantit que les données sensibles ne peuvent pas être lues par une personne extérieure ; le texte transmis est brouillé avec une clé de cryptage ou des clés de cryptage multiples et ne peut être décodé qu'avec la clé secrète prédéfinie.

En plus de ces services de base, IPSec inclut divers mécanismes d'authentification et de protection contre les attaques par retransmission des données (replay attacks) et de refus de service ( DOS - Denial-Of-Service). Ensemble, ces services constituent l'infrastructure permettant à une entreprise d'utiliser un moyen de communication non sécurisé, comme Internet, pour transférer en toute sécurité des informations sensibles.

## Configuration de réseaux privés virtuels (VPN - Virtual Private Networks)

Le Firewall/VPN Symantec prend en charge deux types de modèles VPN : de passerelle à passerelle et de client à passerelle (200R uniquement). Les tunnels passerelle/passerelle protègent des sous-réseaux entiers. Par exemple, ils peuvent servir à connecter des filiales à un siège social par l'intermédiaire d'Internet, ce qui évite donc de recourir à des lignes spécialisées coûteuses.

L'utilisation des tunnels VPN client/passerelle du Firewall/VPN 200R Symantec permet aux travailleurs itinérants ou distants de se connecter en toute sécurité au réseau du siège de l'entreprise par l'intermédiaire d'Internet. Ce modèle limite les frais associés aux pools de modems et aux coûteux numéros 800, car les employés peuvent utiliser un FAI (fournisseur d'accès Internet) avec un numéro d'appel local pour se connecter de manière transparente au réseau du siège de l'entreprise.

Le Firewall/VPN Symantec fournit les cryptages IPsec suivants:

| | |
|---|---|
| AH MD5 | ESP 3DES |
| AH SHA1 | ESP 3DES MD5 |
| ESP DES | ESP 3DES SHA1 |
| ESP DES MD5 | ESP MD5 |
| ESP DES SHA1 | ESP SHA1 |

**Table 5-1 : Cryptages IPSec**

Le Firewall/VPN Symantec prend en charge deux types de tunnels VPN, à clé statique et à clé dynamique.

- **VPN – Tunnel à clé statique** - Un utilisateur indique manuellement une clé d'authentification (longue chaîne de chiffres et de lettres) ainsi qu'une clé de cryptage (autre chaîne utilisée pour l'algorithme de cryptage) si le cryptage est utilisé. Les clés doivent correspondre des deux côtés du VPN. Un SPI (Security Parameter Index – Index de paramètre de sécurité) est indiqué manuellement et ajouté à tous les paquets transmis entre les passerelles. Le SPI est un identifiant unique permettant à la passerelle d'identifier l'ensemble de clés appartenant à chaque paquet.

- **VPN – Tunnel à clé dynamique** - IKE (Internal Key Exchange – Echange de clés internes) génère automatiquement des clés d'authentification et de cryptage. Généralement, un long mot de passe (désigné "secret partagé") est indiqué. La passerelle doit reconnaître ce mot de passe pour que l'authentification réussisse. Si le secret partagé correspond, des clés SPI, d'authentification et de cryptage sont automatiquement générées et le tunnel est créé. La passerelle "régénère la clé" (elle génère une nouvelle clé) à des intervalles prédéfinis, pour renforcer l'intégrité de la clé.

# Pour configurer un VPN à clé statique

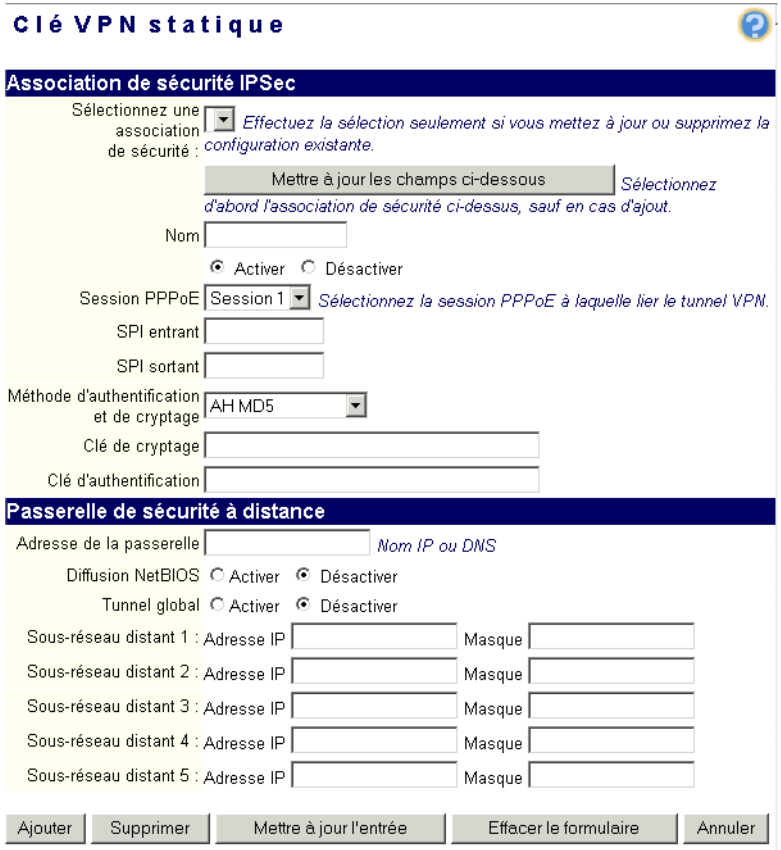



**Figure 5-1 : Ecran VPN – Clé statique**

1. Dans le menu principal, sélectionnez **VPN – Clé statique**.

2. Dans le champ Nom, saisissez un nom décrivant l'Association de sécurité.

   La longueur du nom de l'Association de sécurité doit être comprise entre 1 et 15 caractères.

3. Cliquez sur le bouton radio **Activer**.

4. Dans la liste déroulante Réseau étendu, sélectionnez un port de réseau étendu (VPN 200 uniquement).

5. Dans la liste déroulante **Session PPPoE**, sélectionnez un numéro de session.

   Utilisez Session 1 si vous n'avez qu'une session disponible auprès de votre FAI.

6. Dans le champ **SPI entrant**, indiquez votre index de paramètre de sécurité entrant.

   Le SPI est un nombre hexadécimal (0-9, A-F) ou un nombre décimal. Utilisez le préfixe 0X pour les nombres hexadécimaux.

7. Dans le champ **SPI sortant**, indiquez votre index de paramètre de sécurité sortant.

   Le SPI est un nombre hexadécimal (0-9, A-F) ou un nombre décimal. Utilisez le préfixe 0X pour les nombres hexadécimaux.

8. Dans la liste déroulante **Méthode d'authentification et de cryptage**, sélectionnez la méthode de cryptage.

9. Dans le champ **Clé de cryptage**, saisissez votre clé de cryptage.

   La clé de cryptage doit comporter au minimum 8 caractères ou 16 chiffres hexadécimaux pour DES et 24 caractères ou 48 chiffres hexadécimaux pour 3DES.

10. Dans le champ **Clé d'authentification**, saisissez votre clé d'authentification.

    La clé d'authentification doit comporter au minimum 16 caractères ou 32 chiffres hexadécimaux pour MD5 et 20 caractères ou 40 chiffres hexadécimaux pour SHA1.

11. Dans le champ **Adresse de la passerelle**, saisissez l'adresse de la passerelle du réseau de destination.

    Le format de l'adresse de la passerelle est un minimum de sept chiffres (x.x.x.x) et un maximum de quinze chiffres (xxx.xxx.xxx.xxx). Pour le client VPN, saisissez 0.0.0.0. Vous pouvez aussi utiliser un nom DNS dans le champ **Adresse de la passerelle**.

12. Dans le champ **Diffusion NetBIOS**, sélectionnez l'option **Activer** pour activer la retransmission des paquets de diffusion Netbios.

    Activez cette option pour prendre en charge le Voisinage réseau de Windows à travers un tunnel VPN.

13. Dans le champ **Adresse IP (Sous-réseau distant 1)**, saisissez l'adresse IP du réseau de destination.

14. Dans le champ **Masque (Sous-réseau distant 1)**, saisissez le masque de sous-réseau du réseau de destination.

    Le format du champ du masque de réseau de destination est un minimum de sept chiffres (x.x.x.x) et un maximum de quinze chiffres (xxx.xxx.xxx.xxx).

    Si vous avez plusieurs réseaux distants, répétez les deux premières étapes pour chaque réseau de destination.

15. Cliquez sur **Ajouter** pour enregistrer vos informations de VPN à clé statique et créer votre tunnel VPN statique.

## Pour mettre à jour une configuration de VPN à clé statique

1. Dans le menu principal, sélectionnez **VPN – Clé statique**.

2. Dans la liste déroulante des associations de sécurité, sélectionnez l'Association de sécurité dont vous souhaitez visualiser les informations.

3. Cliquez sur **Mettre à jour les champs ci-dessous**.

4. Indiquez les informations nécessaires.

5. Cliquez sur le bouton **Mettre à jour l'entrée** pour enregistrer vos changements et mettre à jour le **VPN**.

## Pour supprimer une configuration de VPN à clé statique

1. Dans le menu principal, sélectionnez **VPN – Clé statique**.

2. Dans la liste déroulante des associations de sécurité, sélectionnez l'Association de sécurité dont vous souhaitez visualiser les informations.

3. Cliquez sur **Supprimer** pour supprimer le VPN.

## Exemple de tunnel statique

Dans l'exemple suivant, un diagramme illustre un tunnel statique entre passerelles. Le tableau ( *Table 5-2 à la page 5-7* ) décrit les entrées requises pour configurer les deux extrémités de ce tunnel statique.

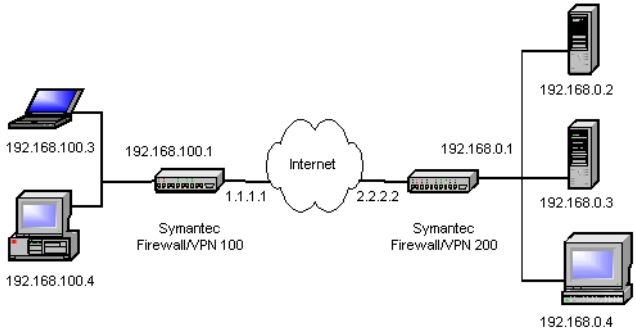



**Figure 5-2 : Diagramme de tunnel statique**

**Table 5-2 : Exemples de paramètres de réseau pour un tunnel statique**

| Champs de l'écran VPN – Clé statique | Paramètres du FW/VPN 100 Symantec | Paramètres du FW/VPN 200 Symantec |
|---|---|---|
| **Association de sécurité IPSec** | | |
| Nom | static_100_to_200 | static_200_to_100 |
| Activer/Désactiver | Activer | Activer |
| Port de réseau étendu (VPN200 uniquement) | Réseau étendu 1 | Réseau étendu 2 |
| Session PPPoE | Session 1 | Session 1 |
| SPI entrant | 257 | 300 |
| SPI sortant | 300 | 257 |
| Méthode d'authentification et de cryptage | ESP DES MD5 | ESP DES MD5 |
| Clé de cryptage | 0X1234567890123456 | 0X1234567890123456 |
| Clé d'authentification | 0X12345678901234567890123456789012 | 0X12345678901234567890123456789012 |
| **Passerelle de sécurité à distance :** | | |
| Adresse de la passerelle | 2.2.2.2 | 1.1.1.1 |
| Diffusion NetBIOS | Désactiver | Désactiver |
| Tunnel global | Désactiver | Désactiver |
| IP sous-réseau distant 1 | 192.168.0.0 | 192.168.100.0 |
| Masque sous-réseau distant 1 | 255.255.255.0 | 255.255.255.0 |

# Pour configurer un VPN à clé dynamique

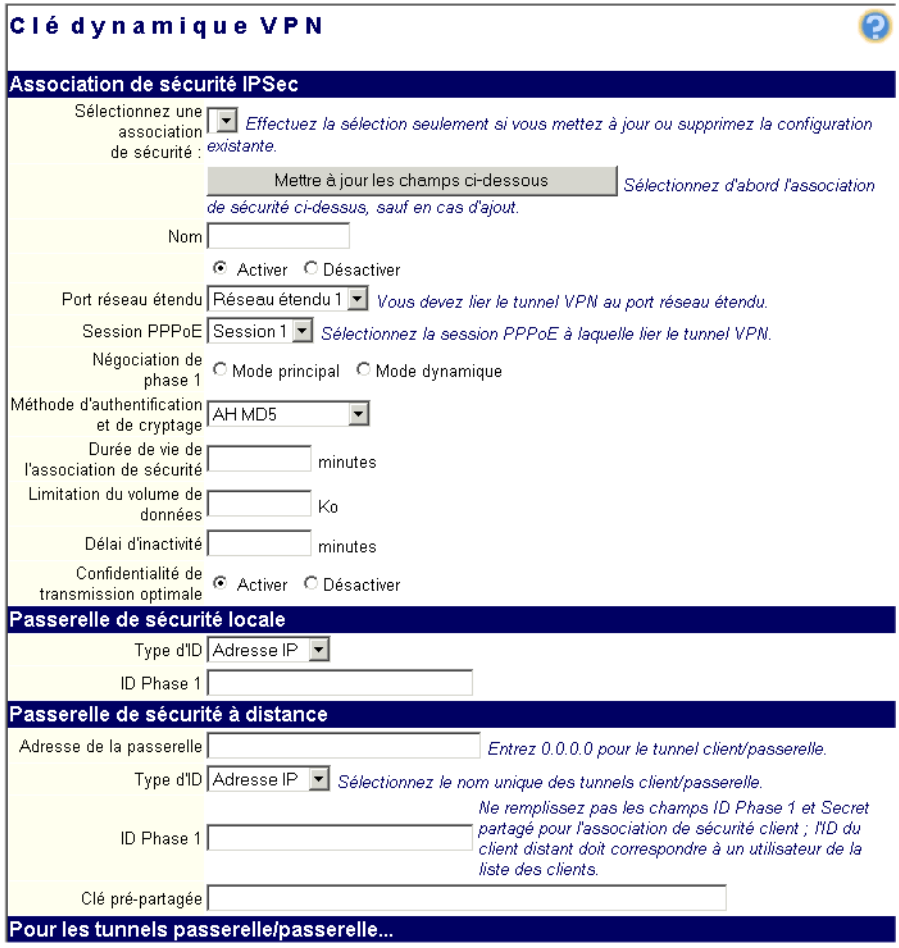



**Figure 5-3 : Ecran VPN – Clé dynamique, partie 1**

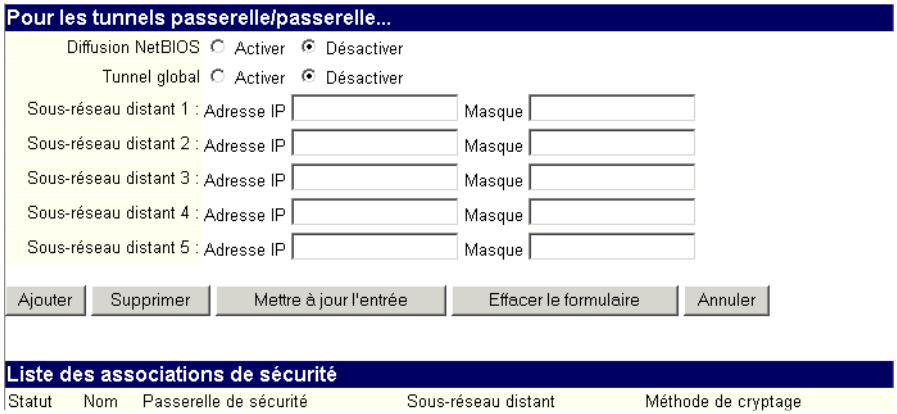



**Figure 5-4 : Ecran VPN – Clé dynamique, partie 2**

1. Dans le menu principal, sélectionnez **VPN – Clé dynamique**.

2. Dans le champ Nom, saisissez un nom décrivant l'Association de sécurité.

3. Cliquez sur le bouton radio **Activer**.

4. Dans la liste déroulante Réseau étendu, sélectionnez un port de réseau étendu.

5. Dans la liste déroulante **Session PPPoE**, sélectionnez le numéro de session.

   Utilisez Session 1 si vous n'avez qu'une session disponible auprès de votre FAI.

6. Cliquez sur le bouton radio **Mode principal** ou **Mode dynamique** pour activer la négociation de phase 1.

   Le **Mode principal** utilise un échange de six messages pour valider l'identité de l'initiateur et du répondant. Par défaut, le mode principal utilise les adresses IP pour identifier les passerelles VPN. Néanmoins, cela peut être remplacé par une étiquette de texte si l'adresse de la passerelle est convertie par NAT sur le réseau. Le mode principal fournit la meilleure protection contre les attaques DOS (Denial Of Service) basées sur le cryptage.

Le **Mode dynamique** échange trois messages entre l'initiateur et le répondant pendant la négociation de clé. Ce mode ne dépend pas de l'adresse IP des deux périphériques et il est donc souvent utilisé pour les tunnels VPN où l'adresse IP n'est pas connue d'avance. Par exemple, les utilisateurs itinérants ont généralement une adresse IP dynamique délivrée par leur FAI ; dans ce mode, rien d'autre n'est nécessaire pour identifier l'émetteur de la requête. En général, dans les configurations client/passerelle, l'identification se fait par l'ID utilisateur.

7. Dans la liste déroulante Méthode d'authentification et de cryptage, sélectionnez la méthode de cryptage.

8. Dans le champ Durée de vie de l'association de sécurité, indiquez la durée en minutes pendant laquelle l'Association de sécurité doit rester active avant de régénérer automatiquement les clés.

9. Dans le champ Limitation du volume de données de l'association de sécurité, indiquez la quantité de données en kilo-octets pouvant traverser le VPN avant que l'Association de sécurité ne régénère automatiquement les clés.

10. Dans le champ Délai d'inactivité, indiquez le délai d'inactivité en secondes au bout duquel le VPN sera fermé automatiquement.

11. Dans le champ **Confidentialité de transmission optimale**, sélectionnez **Activer** ou **Désactiver** pour définir la confidentialité de transmission optimale sur un échange Diffie-Hellman en phase 2 IKE.

12. Dans le champ, Passerelle de sécurité locale, liste déroulante Type d'ID, sélectionnez ID pour la négociation de phase 1 IKE : **Adresse IP** ou **Nom unique**.

13. Dans le champ ID phase 1, indiquez la valeur ou le nom de l'ID phase 1.

    Quand le type Adresse IP est sélectionné, la valeur par défaut est l'adresse IP de la passerelle.

14. Sous la section Passerelle de sécurité à distance, dans le champ **Adresse de la passerelle**, saisissez l'adresse de la passerelle du réseau de destination.

    L'adresse de la passerelle peut être une adresse IP ou le nom DNS de la passerelle distante. La valeur 0.0.0.0 est réservée pour les configurations client/passerelle.

15. Dans le champ Clé pré-partagée, saisissez votre Clé pré-partagée.

    La Clé pré-partagée est une clé prédéfinie utilisée par les deux extrémités d'un tunnel VPN pour s'identifier entre elles.

    La Clé pré-partagée doit comporter au minimum 20 caractères et au maximum 64 caractères.

16. Sous la section Pour les tunnels passerelle/passerelle, cliquez sur le bouton radio **Activer diffusion NetBIOS** pour activer la retransmission des paquets de diffusion Netbios.

17. Cliquez sur le bouton radio **Activer** ou **Désactiver** Tunnel global.

    En activant l'option Tunnel global pour un tunnel VPN, tout le trafic sortant (Internet) passe par le tunnel VPN. Cela est utile pour les stratégies de sécurité qui imposent le passage de tous les trafics internes par une passerelle centralisée.

18. Dans le champ **Adresse IP (Sous-réseau distant 1)**, saisissez l'adresse IP du réseau de destination.

    Le format de l'adresse de la passerelle est un minimum de sept chiffres (x.x.x.x) et un maximum de quinze chiffres (xxx.xxx.xxx.xxx).

19. Dans le champ **Masque (Sous-réseau distant 1)**, saisissez le masque de sous-réseau de votre sous-réseau distant.

    Si vous avez plusieurs sous-réseaux distants, répétez les deux premières étapes pour chaque sous-réseau de destination.

20. Cliquez sur **Ajouter** pour enregistrer vos informations de VPN à clé dynamique et créer votre VPN.

## Pour mettre à jour une configuration de VPN à clé dynamique

1. Dans le menu principal, sélectionnez **VPN – Clé dynamique**.

2. Dans la liste déroulante des associations de sécurité, sélectionnez l'Association de sécurité dont vous souhaitez visualiser les informations.

3. Cliquez sur **Mettre à jour les champs ci-dessous**.

4. Indiquez les informations nécessaires.

5. Cliquez sur le bouton **Mettre à jour l'entrée** pour enregistrer vos changements et mettre à jour le **VPN**.

## Pour supprimer une configuration de VPN à clé dynamique

1. Dans le menu principal, sélectionnez **VPN – Clé dynamique**.

2. Dans la liste déroulante des associations de sécurité, sélectionnez l'Association de sécurité dont vous souhaitez visualiser les informations.

3. Cliquez sur **Supprimer** pour supprimer le VPN.

## Exemple de tunnel dynamique

L'exemple suivant se compose d'un diagramme réseau représentant un tunnel dynamique passerelle/passerelle et un tableau (*Table 5-3 à la page 5-13*) décrivant les entrées requises pour configurer les deux extrémités de ce tunnel dynamique.

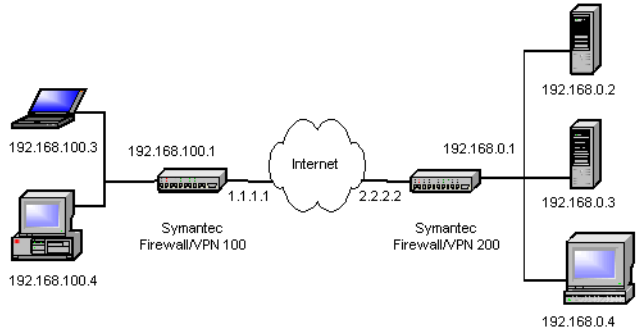



**Figure 5-5 : Exemple de tunnel dynamique**

**Table 5-3 : Exemples de paramètres réseau pour tunnel dynamique**

| Champs de l'écran VPN – Clé dynamique | Paramètres du FW/VPN 100 Symantec | Paramètres du FW/VPN 200 Symantec |
|---|---|---|
| **Association de sécurité IPSec** | | |
| Nom | dynamicIKE_100_to_200 | dynamicIKE_200_to_100 |
| Activer/Désactiver | Activer | Activer |
| Port de réseau étendu (VPN200 uniquement) | Réseau étendu 1 | Réseau étendu 2 |
| Session PPPoE | Session 1 | Session 1 |
| Négociation de phase 1 | Mode principal | Mode principal |
| Méthode d'authentification et de cryptage | ESP DES MD5 | ESP DES MD5 |
| Durée de vie de l'association de sécurité | 0 (0 signifie aucune limitation) | 0 (0 signifie aucune limitation) |
| Limitation du volume de données | 0 (0 signifie aucune limitation) | 0 (0 signifie aucune limitation) |
| Délai d'inactivité | 0 (0 signifie aucune limitation) | 0 (0 signifie aucune limitation) |
| Confidentialité de transmission optimale | Activer | Activer |
| **Passerelle de sécurité locale :** | | |
| Type d'ID | Adresse IP | Adresse IP |
| ID phase 1 | vide | vide |
| **Passerelle de sécurité à distance :** | | |
| Adresse de la passerelle | 2.2.2.2 | 1.1.1.1 |
| Type ID | Adresse IP | Adresse IP |

| Champs de l'écran VPN – Clé dynamique | Paramètres du FW/VPN 100 Symantec | Paramètres du FW/VPN 200 Symantec |
|---|---|---|
| ID phase 1 | vide | vide |
| Clé pré-partagée | everygoodboydoesfine | everygoodboydoesfine |
| **Pour les tunnels passerelle/passerelle :** | | |
| Diffusion NetBIOS | désactiver | désactiver |
| Tunnel global | désactiver | désactiver |
| IP de sous-réseau distant 1 | 192.168.0.0 | 192.168.100.0 |
| Masque sous-réseau distant 1 | 255.255.255.0 | 255.255.255.0 |

# VPN – Identité du client

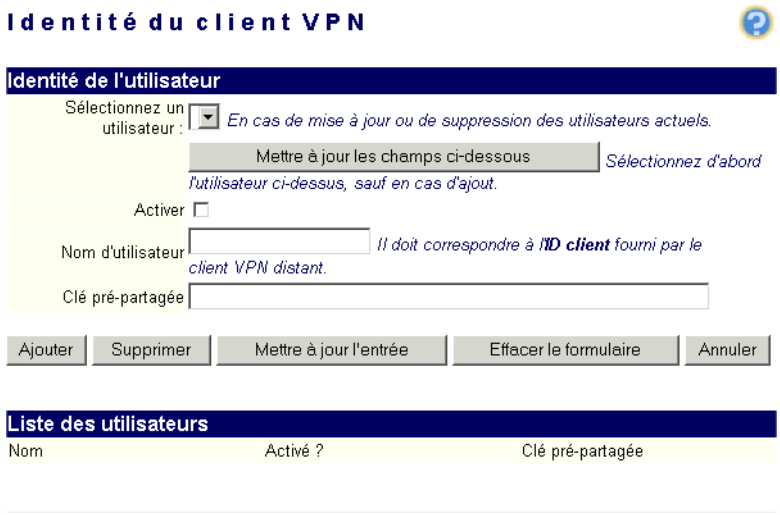



**Figure 5-6 : Ecran VPN – Identité du client**

L'écran VPN – Identité du client identifie et valide les utilisateurs du Client VPN. Il permet aussi de définir les Clés pré-partagées.

**Pour ajouter un nouvel utilisateur du Client VPN**

1. Dans le menu principal du Firewall/VPN 200R Symantec, sélectionnez **Identité du client**.
2. Dans la section Identité du client, cliquez sur **Activer**.
3. Dans le champ Nom d'utilisateur, saisissez votre nom d'utilisateur.
4. Dans le champ Clé pré-partagée, saisissez votre clé pré-partagée.

   La clé pré-partagée doit comprendre entre 20 et 64 caractères.
5. Cliquez sur **Ajouter**.

# Chapitre 6

# Utilitaires

## Sauvegarde/Analogique/RNIS

Cet écran vous permet de configurer les informations de secours automatique ou de connexion analogique/RNIS. Vous devez connecter un modem externe (analogique ou RNIS) au port série du Firewall/VPN pour utiliser cette fonctionnalité. En mode Sauvegarde, le Firewall/VPN Symantec établit automatiquement une connexion si la liaison large bande tombe en panne. Il réactive aussi automatiquement la connexion large bande quand celle-ci est de nouveau disponible. Vous pouvez aussi déclencher manuellement la connexion Analogique/RNIS.

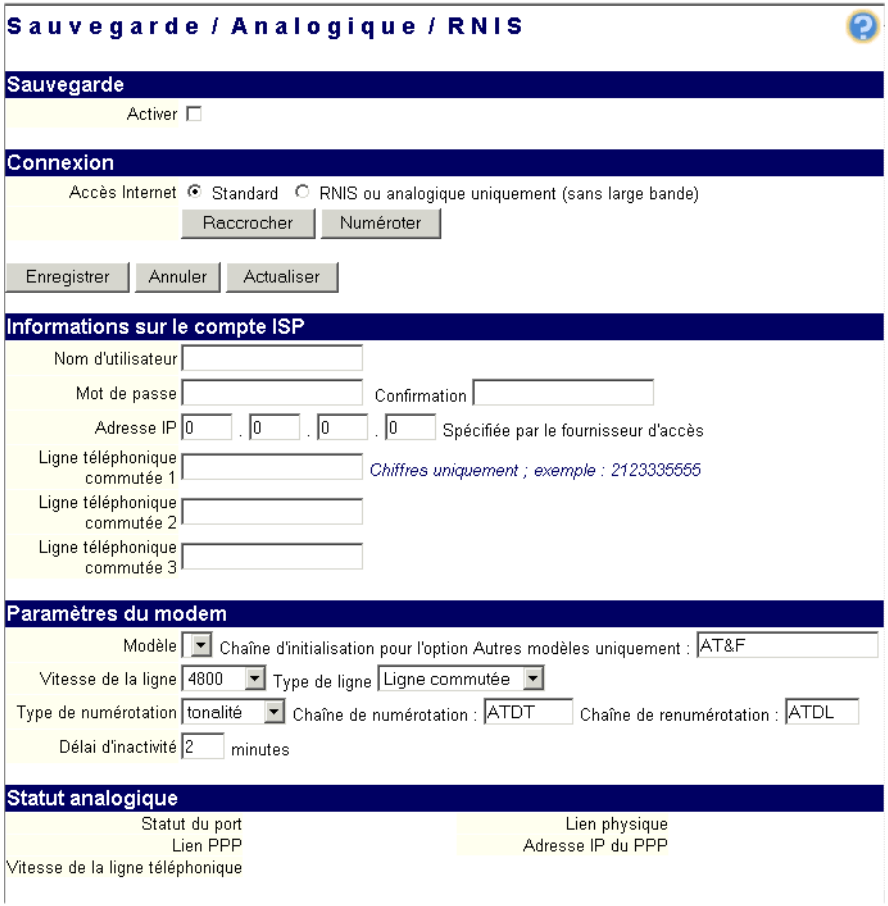



**Figure 6-1 : Ecran Sauvegarde/Analogique/RNIS**

Si votre connexion Internet est de type DHCP dynamique ou IP statique, l'Indicateur d'activité doit être configuré. L'Indicateur d'activité est utilisé par le Firewall/VPN pour déterminer si une connexion réseau étendu fonctionne, même s'il n'y a aucun trafic sur le réseau étendu (nécessaire pour l'activation de la sauvegarde). Toutes les 20 secondes, l'unité contacte la passerelle ou le DNS du FAI (fournisseur d'accès Internet) pour déterminer s'il est connecté. Cela fonctionne normalement, sauf avec certains FAI qui interdisent d'interroger leurs passerelles. Indiquez un nom de domaine ou une adresse IP dans ce champ pour qu'une interrogation supplémentaire soit effectuée si la passerelle ne répond pas (n'utilisez pas le préfixe http://). Effectuez d'abord un "ping" manuel. Non utilisé pour PPPoE.

**Pour configurer la fonction Sauvegarde/Analogique/RNIS**

1. Dans la section Sauvegarde, cochez la case **Activer**.

   Quand cette option est activée, le Firewall/VPN Symantec se connecte automatiquement si la connexion large bande ne fonctionne plus.

2. Dans la section Connexion, dans les champs Accès Internet, cochez la case Standard, RNIS ou analogique uniquement (sans large bande) pour identifier le type de connexion.

3. Cliquez sur **Raccrocher** ou sur **Numéroter** pour vous connecter et déconnecter manuellement à votre compte d'accès analogique.

**Remarque :** Cliquez toujours sur **Enregistrer** après avoir modifié des paramètres.

4. Dans la section Informations sur le compte FAI, indiquez les informations de compte Analogique ou RNIS fournies par votre FAI.

   a. Dans le champ Nom d'utilisateur, saisissez le nom d'utilisateur de votre compte d'accès analogique ou RNIS.

   b. Dans le champ Mot de passe, saisissez le mot de passe de votre compte d'accès analogique ou RNIS.

   c. Dans le champ Confirmation, saisissez de nouveau le mot de passe de votre compte d'accès analogique ou RNIS.

   d. Dans le champ Adresse IP, saisissez votre adresse IP.

      Consultez votre FAI pour obtenir l'adresse IP.

   e. Dans le champ Numéro de téléphone d'accès n°1, saisissez le numéro de téléphone d'accès de votre FAI, sans espaces ni tirets.

      Vous pouvez indiquer jusqu'à 3 numéros de téléphone à composer si le premier est occupé.

5. Dans la section Paramètres du modem, indiquez les informations de votre modem.

   a. Dans la liste déroulante Modem, sélectionnez le type de votre modem.

      Pour déterminer les meilleurs paramètres à utiliser, consultez le manuel d'utilisation de votre modem. Plusieurs modems sont prédéfinis. Si votre modem n'apparaît pas dans la liste, sélectionnez l'option Autres et saisissez la chaîne d'initialisation de votre modem. Si vous ne savez pas comment faire, consultez le constructeur de votre modem.

   b. Dans la liste déroulante Vitesse de la ligne, sélectionnez la vitesse de la connexion à votre FAI (fournisseur d'accès Internet).

      Si vous avez des problèmes pour vous connecter, diminuez la vitesse de la ligne.

   c. Dans la liste déroulante Type de ligne téléphonique, sélectionnez le type de votre ligne.

      Le type de ligne est généralement Connexion à distance mais vous pouvez sélectionner l'option Ligne spécialisée si cela correspond à votre installation.

   d. Type et Chaînes de numérotation

      Ne modifiez ces paramètres que si vous n'avez pas de tonalité. Pour modifiez les chaînes de numérotation, consultez le manuel d'utilisation de votre modem.

      Dans le champ Délai d'inactivité, saisissez le délai d'inactivité en minutes si vous voulez vous déconnecter automatiquement de votre compte analogique/RNIS après une période d'inactivité.

      Indiquez 0 pour que le modem reste connecté en permanence.

Le champ Statut analogique fournit des informations utiles pour l'assistance technique en cas de problème avec votre connexion PPP (analogique/RNIS).

# Console de configuration série

Le Firewall/VPN Symantec peut être configuré ou réinitialisé au travers du port série, en utilisant le câble "Null Modem" inclus, raccordé au port COM d'un ordinateur. Cette console de configuration est très utile pour installer le Firewall/VPN Symantec sur un réseau existant. Cela évite que le Firewall/VPN Symantec n'interfère avec le réseau quand il est connecté. Avec la console de configuration série vous pouvez :

- Modifier l'adresse IP locale (la valeur par défaut est 192.168.0.1)
- Modifier le masque de réseau local
- Désactiver/activer le serveur DHCP (activé par défaut)
- Modifier l'IP de début et de fin pour la plage d'IP du serveur DHCP

**Pour utiliser la console série**

1. Connectez le câble Null Modem entre le port COM de votre ordinateur et le port série du Firewall/VPN.
2. Basculez le micro-commutateur 3 sur **ON** (vers le bas) sur le Firewall/VPN.
3. Lancez un programme de gestion de terminal (HyperTerminal est inclus avec Windows).
4. Configurez-le pour qu'il se connecte directement à votre port COM (en général COM1 ou COM2).
5. Vous devez définir les paramètres de communication de la manière suivante pour vous connecter au Firewall/VPN.

| | |
|---|---|
| Baud<br>(Bits par seconde) | 9600 |
| Bits de données | 8 |
| Parité | Sans |
| Bits d'arrêt | 1 |
| Contrôle de flux | Sans |

6. Une fois le terminal connecté avec les paramètres ci-dessus, appuyez sur le bouton **Réinitialiser** sur le Firewall/VPN. L'écran de la console doit apparaître.

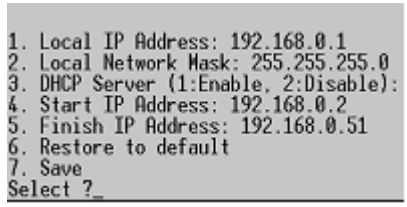



**Figure 6-2 : Ecran de la console**

7. Effectuez vos sélections et veillez à sélectionner **SAVE (7)** pour enregistrer après avoir terminé.

8. Basculez le micro-commutateur 3 sur **OFF** (vers le haut) après avoir utilisé la console.

## Réinitialisation manuelle

Un paramétrage incorrect sur l'écran IP locale & DHCP ou l'oubli de votre mot de passe de configuration peuvent vous empêcher d'accéder à l'unité. Le fait d'appuyer sur le bouton **Réinitialiser** de l'unité ne restaurera pas les paramètres IP par défaut et ne désactivera pas le mot de passe. Vous devez effectuer les étapes suivantes pour pouvoir de nouveau vous connecter au Firewall/VPN.

Cette procédure effectue les tâches suivantes :

- Restaure l'adresse IP de l'unité à sa valeur par défaut : 192.168.0.1
- Restaure le masque de réseau de l'unité à sa valeur par défaut : 255.255.255.0
- Efface le mot de passe de l'interface.
- Active le Serveur DHCP

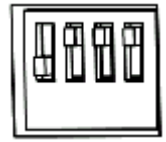
**Pour réinitialiser manuellement le Firewall/VPN Symantec**

**Remarque :** Lisez l'ensemble de ces étapes avant de commencer la réinitialisation du Firewall/VPN.

**Remarque :** Un trombone est nécessaire pour cette procédure.

1. Coupez l'alimentation du Firewall/VPN Symantec en débranchant le câble électrique à l'arrière de l'unité.

2. Basculez le micro-commutateur 1 sur **ON** (vers le bas).



3. Réinsérez le connecteur d'alimentation dans la prise de l'unité et ATTENDEZ 4 SECONDES.

4. Ensuite, sans vous interrompre, basculez le micro-commutateur 1 sur **OFF** (VERS LE HAUT).

5. Basculez le micro-commutateur 1 sur **ON** (VERS LE BAS).

6. Basculez le micro-commutateur 1 sur **OFF** (VERS LE HAUT).

   Cette séquence de redémarrage doit se faire dans les 10 secondes suivant la mise sous tension du Firewall/VPN.

7. Quand les voyants d'activité du réseau local clignotent et que la séquence de réinitialisation recommence, l'unité est réinitialisée.

8. Retirez le câble d'alimentation.

9. Attendez quelques instants, puis rebranchez le câble d'alimentation.

Il est important de ne pas basculer le commutateur trop vite. Utilisez des mouvements lents et réguliers. Entraînez-vous pour l'étape 4 avec l'alimentation débranchée avant d'essayer pour la première fois.

L'unité doit avoir de nouveau ses valeurs par défaut pour l'IP et le masque de réseau et le mot de passe doit être effacé.

## Sauvegarde de la configuration

Le Firewall/VPN Symantec vous permet de sauvegarder les paramètres de configuration définis par l'intermédiaire de l'interface utilisateur, pour le cas où l'unité aurait un problème. Cette procédure produit un petit fichier qui peut être copié sur une disquette et rangé dans un coffre ou autre endroit sûr.

Pour effectuer ces étapes, vous devez vous servir de l'utilitaire "nxtftpw". Il y a deux versions de l'utilitaire "nxtftpw"; une version Windows (Win95/98/ME/NT & 2000) et une version DOS. Les deux sont présentes sur le CD, dans le répertoire Utilities. La procédure suivante utilise la version Windows.

**Pour récupérer le fichier de sauvegarde**

1. Coupez l'alimentation de l'unité en débranchant le câble électrique à l'arrière du Firewall/VPN.

2. Basculez les micro-commutateurs 1 et 2 en position **ON** (VERS LE BAS).

3. Réinsérez le connecteur d'alimentation dans la prise du Firewall/VPN.

4. Copiez l'utilitaire nxtftpw du CD vers un dossier de votre disque dur.

5. Cliquez deux fois sur l'icône de nxtftpw.

6. Indiquez l'adresse IP du Firewall/VPN Symantec dans le champ IP du serveur (l'adresse est 192.168.0.1, sauf si vous l'avez changée).

7. Indiquez un nom pour le fichier de sauvegarde dans le champ Fichier local (vous pouvez utiliser "config").

8. Cliquez sur le bouton **Get**.

   Après quelques instants; un fichier dénommé config va apparaître dans le même dossier que l'application nxtftpw. Vous pouvez copier ce fichier sur une disquette pour le conserver en lieu sûr.

9. Vous pouvez maintenant remettre les micro-commutateurs 1 et 2 en position **OFF**.

# Affichage du journal

Les écrans Affichage du journal du Firewall/VPN Symantec affichent la liste des événements système.


**Figure 6-3 : Ecran Affichage du journal**

# Paramètres du journal

Cet écran vous permet de définir le type d'entrées de journal enregistrées et les paramètres de retransmission du journal. Les journaux générés sur le Firewall/VPN Symantec sont placés dans une mémoire tampon de capacité limitée. Quand le journal est plein, les nouvelles entrées remplacent les plus anciennes. Il est donc souhaitable de faire suivre le journal.

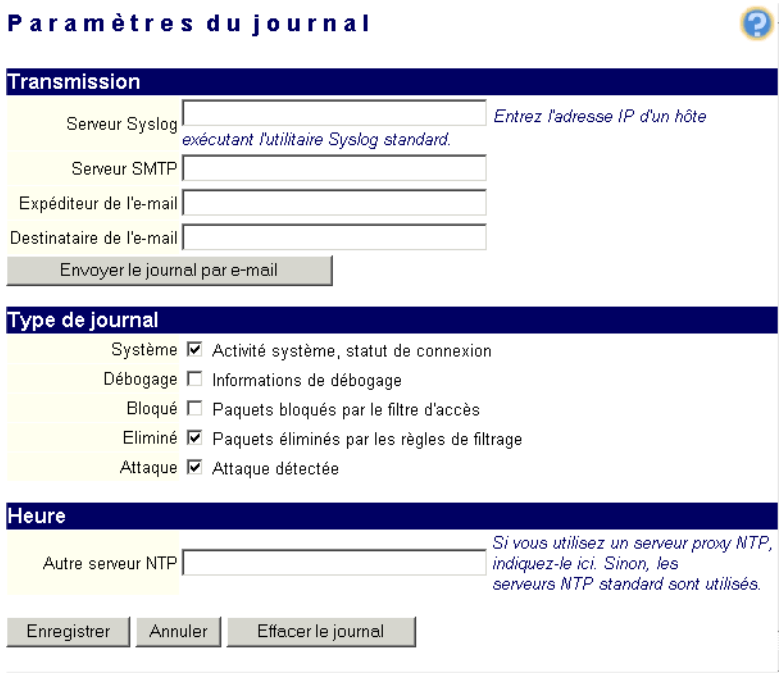



**Figure 6-4 : Ecran Paramètres du journal**

## Pour configurer les paramètres du journal

1. Dans la section Transmission, champ Serveur Syslog, saisissez l'adresse IP d'un hôte exécutant un utilitaire Syslog standard pour recevoir le fichier Journal.

2. Dans le champ Serveur SMTP, saisissez l'adresse IP ou l'URL du serveur SMTP qui doit recevoir le fichier journal dans le champ Serveur SMTP de la section Paramètres e-mail.

3. Dans le champ Expéditeur de l'e-mail, indiquez l'adresse e-mail de l'expéditeur du message.

   Le champ Expéditeur de l'e-mail peut contenir jusqu'à 39 caractères.

4. Dans le champ Destinataire de l'e-mail, indiquez le destinataire de l'e-mail.

   Le champ Destinataire de l'e-mail peut contenir jusqu'à 39 caractères. Si vous voulez spécifier plusieurs destinataires, séparez-les par une virgule.

5. Sous la section **Type de journal**, cochez les cases correspondant aux types de messages que vous voulez consigner.

6. Sous la section Heure, dans le champ Autre serveur NTP, saisissez l'adresse IP d'un autre serveur NTP.

   Si vous utilisez un proxy ou êtes situé derrière un firewall nécessitant une passerelle NTP, indiquez ici son adresse IP. Sinon, les serveurs NTP standard seront utilisés pour obtenir l'heure des entrées de journal.

7. Cliquez sur **Enregistrer**.

# Chapitre 7

# Configuration du Firewall/VPN Symantec pour Symantec Enterprise VPN

Le Firewall/VPN Symantec permet de créer des tunnels entre lui-même et un serveur Symantec Enterprise VPN (SEVPN). Ce tunnel peut être créé statiquement ou dynamiquement avec IKE. Ce chapitre décrit les étapes de création de tunnels statiques et dynamiques.

**Remarque :** Ce chapitre traite uniquement des étapes requises du côté du Firewall/VPN Symantec. Il considère que le SEVPN est déjà configuré et que les informations requises sont disponibles sur cette configuration. Consultez les sections appropriées du *Guide d'installation Symantec Enterprise Firewall et Symantec Enterprise VPN* et du *Guide de configuration de Symantec Enterprise Firewall et Symantec Enterprise VPN* si vous avez besoin d'aide pour configurer le SEVPN.

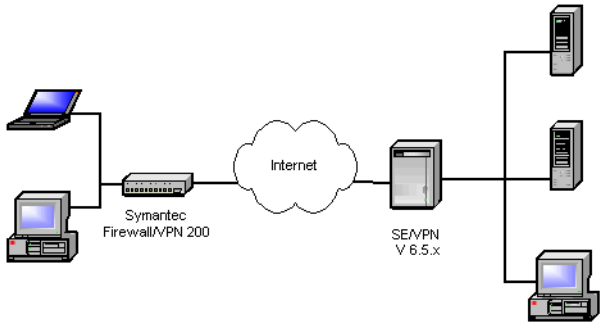



**Figure 7-1 : Connexion du Firewall/VPN Symantec à Symantec Enterprise VPN**

# Tunnel statique

Les tunnels statiques sont configurés en spécifiant toutes les informations essentielles pour les deux extrémités du tunnel. Les deux extrémités doivent se correspondre exactement pour que le tunnel fonctionne correctement. Les tunnels statiques peuvent utiliser un encapsulage de force DES ou 3DES.

## Configuration de tunnel statique avec le Firewall/VPN Symantec

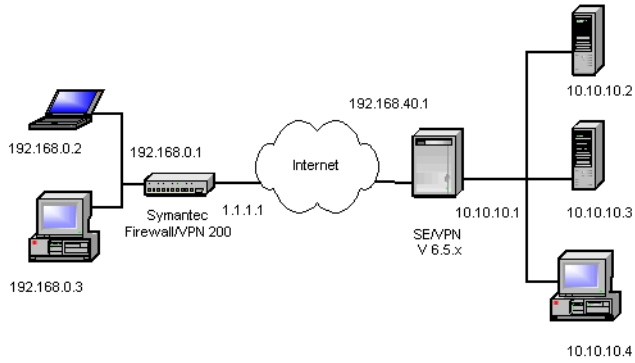



**Figure 7-2 : VPN - Diagramme de tunnel statique**

Sur l'application du Firewall/VPN Symantec, sélectionnez l'option **VPN - Statique** dans la page de configuration. Vous devez obtenir un écran similaire à la *Figure 7-3 à la page 7-3*.

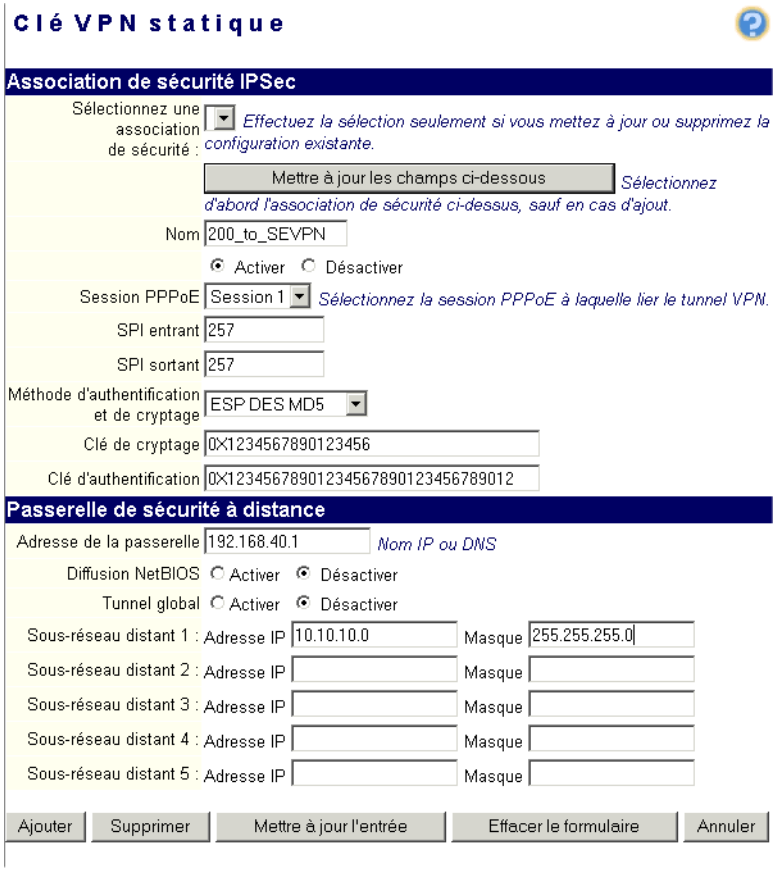



**Figure 7-3 : Ecran de configuration de VPN statique**

Initialement, l'écran ne contient que quelques paramètres par défaut. Pour configurer un tunnel statique, vous aurez besoin des informations suivantes sur le SEVPN :

- Adresse IP de la passerelle du SEVPN.
- Destination réseau protégée par le SEVPN.
- Masque de réseau du réseau distant protégé par le SEVPN.
- SPI local

- SPI distant
- Paramètres de cryptage sur le SEVPN (DES, 3DES, SHA1, etc.)
- Clé d'algorithme de confidentialité
- Clé d'algorithme d'intégrité

Pour configurer le tunnel

1. Dans le champ **Nom**, indiquez un nom pour ce tunnel.
2. Cliquez sur **Activer**.
3. Sélectionnez le **Port de réseau étendu** auquel vous souhaitez lier le tunnel VPN. (VPN 200 uniquement)
4. Sélectionnez la **Session PPPoE** à laquelle vous souhaitez lier le tunnel.
5. Définissez le **SPI entrant** en fonction du SPI distant du SEVPN.
6. Définissez le **SPI sortant** en fonction du SPI local du SEVPN.
7. Sélectionnez la **Méthode d'authentification et de cryptage** en fonction des paramètres du SEVPN.
8. Définissez la **Clé de cryptage** en fonction de la clé d'algorithme de confidentialité du SEVPN. Si vous utilisez 3DES vous devrez concaténer les trois clés du SEVPN pour former une clé.
9. Définissez la **Clé d'authentification** en fonction de la clé d'algorithme d'intégrité du SEVPN.
10. Définissez l'**Adresse de passerelle** qui sera l'adresse de passerelle du SEVPN.
11. Cochez **Désactiver** pour **Diffusion NetBIOS**.
12. Cochez **Désactiver** pour **Tunnel global**.
13. Définissez **Adresse IP (Sous-réseau distant)** sur le réseau de destination protégé par le SEVPN.

14. Définissez **Masque (Sous-réseau distant)** sur le masque réseau du réseau de destination protégé par le SEVPN.

15. Cliquez sur **Ajouter** pour ajouter le nouveau tunnel au système.

Le tunnel doit à présent être opérationnel aux deux extrémités. Pour le vérifier, ouvrez une ligne de commande DOS et envoyez un ping à une machine du réseau distant.

## Configuration de tunnel statique sur le SEVPN

Le tableau suivant contient une brève liste des étapes de configuration du SEVPN.

| Etapes de configuration | Guide de configuration de Symantec Enterprise Firewall et Symantec Enterprise VPN - Chapitre |
|---|---|
| 1. Créer une **passerelle de sécurité** pour le SEVPN. | Defining Security Gateways |
| 2. Créer un **sous-réseau** pour le SEVPN. | Defining Subnet Entities |
| 3. Créer une **passerelle de sécurité** pour le Firewall/VPN Symantec. | Defining Security Gateways |
| 4. Créer un **sous-réseau** pour le réseau distant. | Defining Subnet Entities |
| 5. Créer un **tunnel sécurisé**, sélectionner l'une des politiques statiques, configurer les clés et définir les SPI. | Configuring Secure Tunnels and Configuring an IPsec Static VPN Policy |

# Tunnel dynamique

Les tunnels dynamiques diffèrent des tunnels statiques dans la mesure où les deux extrémités du tunnel échangent les clés de cryptage dynamiquement. Il n'est pas nécessaire de les configurer à l'avance.

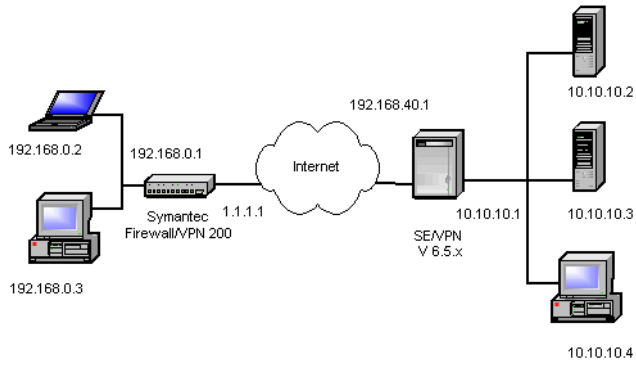



**Figure 7-4 : Diagramme de tunnel dynamique**

## Configuration de tunnel dynamique pour Firewall/VPN 100 Symantec

Sur le Firewall/VPN Symantec, sélectionnez l'option **VPN - Dynamique** dans la page de configuration. Vous devez obtenir un écran similaire à la *Figure 7-5 à la page 7-7*. Initialement, l'écran ne contient que quelques paramètres par défaut. Pour configurer un tunnel dynamique, vous aurez besoin des informations suivantes sur le SEVPN :

- Adresse IP de la passerelle du SEVPN.
- Secret partagé.
- Réseau de destination protégé par le SEVPN.
- Masque du réseau de destination protégé par le SEVPN.
- Paramètres de cryptage sur SEVPN (DES, 3DES, SHA1, etc.)
- Paramètre de confidentialité de transmission optimale.

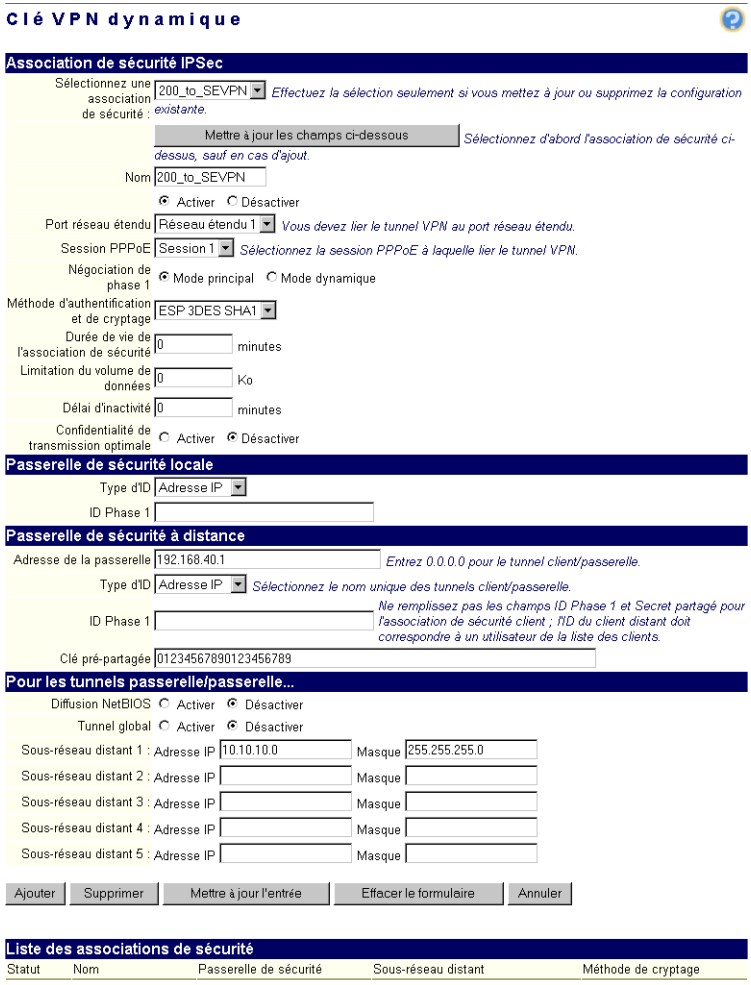



**Figure 7-5 : Ecran de configuration de VPN dynamique**

Pour configurer le tunnel

1. Dans le champ **Nom**, indiquez un nom pour ce tunnel.
2. Cochez **Activer**.
3. Sélectionnez le **Port de réseau étendu** auquel vous souhaitez lier le tunnel VPN.

4. Sélectionnez la **Session PPPoE** à laquelle vous souhaitez lier le tunnel.

5. Cochez **Mode principal** pour **Négociation de phase 1**.

6. Sélectionnez la **Méthode d'authentification et de cryptage** en fonction des paramètres du SEVPN.

7. Cochez l'option **Confidentialité de transmission optimale** en fonction des paramètres du SEVPN.

8. Sous Passerelle de sécurité à distance, définissez l'**Adresse de passerelle** qui sera l'adresse de passerelle du SEVPN.

9. Définissez **Type ID** sur Adresse IP.

10. Définissez la **Clé pré-partagée** comme Secret partagé du SEVPN.

11. Cochez **Désactiver** pour **Diffusion NetBIOS**.

12. Cochez **Désactiver** pour **Tunnel global**.

13. Définissez **Réseau destination 1** sur le réseau de destination protégé par le SEVPN.

14. Définissez **Masque** sur le masque réseau du réseau de destination protégé par le SEVPN.

15. Cliquez sur **Ajouter** pour ajouter le nouveau tunnel au système.

Le tunnel doit à présent être opérationnel aux deux extrémités. Pour le vérifier, ouvrez une ligne de commande DOS et envoyez un ping à une machine du réseau distant. Après quelques instants, la réponse de ping initiale passera en délai dépassé. L'attente correspond à l'échange des clés entre les extrémités du tunnel.

## Configuration de tunnel dynamique SEVPN

Le tableau suivant contient une brève liste des étapes de configuration du SEVPN.

**Table 7-1 : Etapes de configuration de tunnel dynamique SEVPN**

| Etapes de configuration | Guide de configuration de Symantec Enterprise Firewall et Symantec Enterprise VPN - Chapitre |
|---|---|
| 1. Créer une **passerelle de sécurité** pour le SEVPN. | Defining Security Gateways |
| 2. Créer un **sous-réseau** pour le réseau local. | Defining Subnet Entities |
| 3. Créer une **passerelle de sécurité** pour le Firewall/VPN Symantec. | Defining Security Gateways |
| 4. Créer un **sous-réseau** pour le réseau distant. | Defining Subnet Entities |
| 5. Créer un **tunnel sécurisé**, sélectionner l'une des politiques statiques, configurer les clés et définir les SPI. | Configuring Secure Tunnels and Configuring an IPsec Static VPN Policy |

# Chapitre 8

# Connexion au Client Symantec Enterprise VPN

Le  Client Symantec Enterprise VPN permet à un PC distant de transmettre des informations en toute sécurité à un réseau privé protégé par le Firewall/VPN 200R Symantec, par l'intermédiaire d'un tunnel sécurisé sur Internet. Le Client Symantec Enterprise VPN connecte le PC au Firewall/VPN Symantec, qui assure un accès sécurisé au réseau privé. Pour créer un tunnel sécurisé, vous devez configurer les deux extrémités du tunnel. L'une des extrémités est le Firewall/VPN 200R Symantec et l'autre le Client Symantec Enterprise VPN. Les sections suivantes décrivent la configuration des deux terminaisons du tunnel sécurisé entre le Client Symantec Enterprise VPN et le Firewall/VPN 200R Symantec.

Le Client Symantec Enterprise VPN peut également être configuré derrière le Firewall/VPN 200R Symantec. Dans une configuration derrière le Firewall/VPN Symantec, le Client Symantec Enterprise VPN peut valider des tunnels sécurisés qui traversent le Firewall/VPN 200R Symantec pour atteindre des passerelles distantes.

Par défaut, le Firewall/VPN Symantec peut multiplexer plusieurs connexions IPSec directes sur une même adresse IP.

**Remarque :** Vous ne pouvez pas vous connecter par l'intermédiaire d'une connexion IPSec directe à une passerelle VPN qui a été définie localement dans un tunnel VPN.

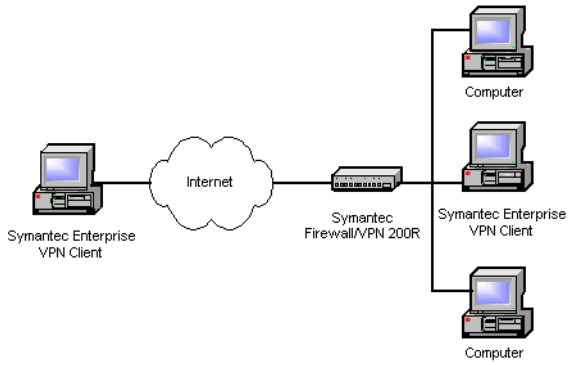



**Figure 8-1 : Configurations du Client Symantec Enterprise VPN**

Pour garantir la transmission sécurisée des données dans les tunnels, le Client Symantec Enterprise VPN utilise un ensemble de protocoles de sécurité standardisés, incluant le protocole ISAKMP (Internet Security Association and Key Management Protocol), la politique IKE (Internet Key Exchange) et le protocole IPSec (IP Security).

L'accès au Client Symantec Enterprise VPN est protégé par mot de passe pour interdire la création non autorisée de tunnels dans le Firewall/VPN 200R Symantec, même si l'ordinateur est volé. Pour renforcer la sécurité, le Client Symantec Enterprise VPN inclut un firewall personnel qui limite les ports sur lesquels les paquets de données peuvent être reçus.

# Configuration du Client Symantec Enterprise VPN avec le Firewall/VPN 200R Symantec

Les passerelles de sécurité doivent être configurées à la fois du côté du Firewall/VPN Symantec et du Client Symantec Enterprise VPN. Chaque passerelle peut prendre en charge des tunnels multiples. En conséquence, quand vous ajoutez ou enlevez une passerelle de sécurité dans la base de données du Client Symantec Enterprise VPN, vous ajoutez ou vous retirez simultanément tous les tunnels associés à la passerelle de sécurité.

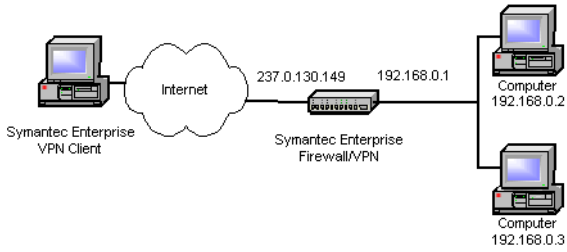



**Figure 8-2 : Configuration de tunnel distant du Client Symantec Enterprise VPN**

Les tunnels doivent être connectés chaque fois que votre PC démarre. Quand les passerelles et les tunnels sont connectés, ils le restent jusqu'à que l'un des événements suivants intervient : une déconnexion volontaire, un dépassement de délai d'inactivité, une perte de connexion, fermeture de Windows ou du Client Symantec Enterprise VPN.

## Configuration du Firewall/VPN 200R Symantec pour un tunnel dynamique vers le Client Symantec Enterprise VPN

1. Dans le menu principal du Firewall/VPN 200R Symantec, sélectionnez **Identité du client**.

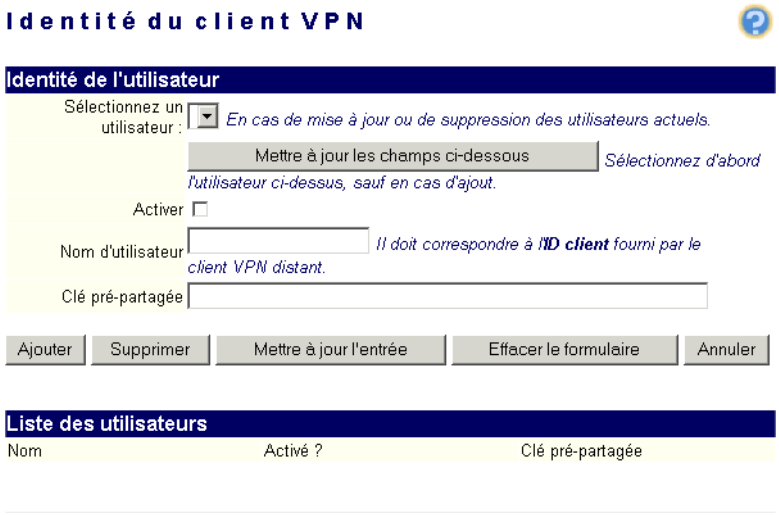



**Figure 8-3 : Ecran Identité du client**

2. Dans la section Identité du client, cliquez sur **Activer**.
3. Dans le champ Nom d'utilisateur, saisissez un nom d'utilisateur.
4. Dans le champ Clé pré-partagée, saisissez votre clé pré-partagée.

   La clé pré-partagée doit comporter entre 20 et 64 caractères.
5. Cliquez sur **Ajouter**.
6. Dans le menu principal du Firewall/VPN 200R Symantec, sélectionnez **Clé VPN dynamique**.
7. Dans la section Association de sécurité IPSec, saisissez un nom décrivant l'Association de sécurité dans le champ Nom.

8. Cliquez sur le bouton radio **Activer** pour activer l'association de sécurité.

9. Dans le champ Négociation de phase 1, cliquez sur le bouton radio **Mode dynamique**.

10. Dans la liste déroulante Méthode de cryptage et d'authentification, sélectionnez une méthode.

    Cette méthode doit correspondre à la méthode de cryptage et d'authentification utilisée pour configurer l'extrémité du tunnel du Client Symantec Enterprise VPN.

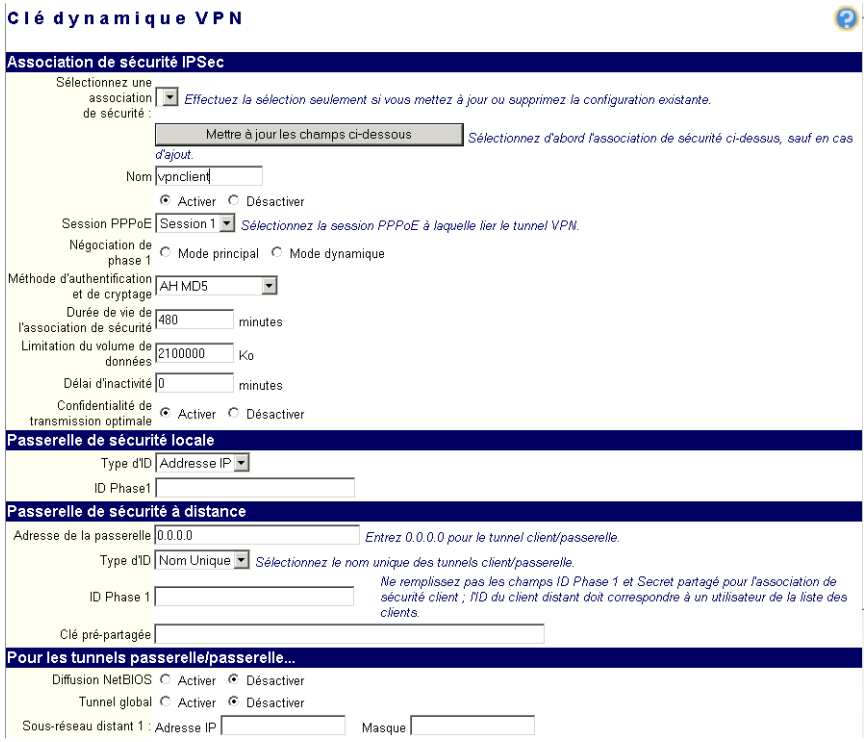



**Figure 8-4 : Ecran VPN – Clé dynamique**

11. Dans le champ Durée de vie de l'association de sécurité, indiquez la durée en minutes pendant laquelle l'association de sécurité doit rester active avant régénération des clés.

Le nombre de minutes de la durée de vie de l'association de sécurité doit correspondre au délai d'expiration du Client Symantec Enterprise VPN tel que saisi sur son écran de politique VPN. Consultez la section *Table 8-1, Configuration du Client Symantec Enterprise VPN à la page 8-7* .

12. Dans le champ Limitation du volume de données de l'association de sécurité, indiquez la quantité de données en kilo-octets pouvant traverser le tunnel avant que l'association de sécurité ne régénère les clés.

    Le nombre de kilo-octets doit correspondre au paramètre indiqué sur l'écran de politique VPN du Client Symantec Enterprise VPN.

13. Dans le champ Délai d'inactivité, indiquez une valeur en minutes.

    Le délai d'inactivité doit correspondre au paramètre indiqué sur l'écran de politique VPN du Client Symantec Enterprise VPN.

14. Cliquez sur le bouton radio **Activer** dans le champ Confidentialité de transmission optimale.

15. Sous la section Passerelle de sécurité à distance, dans le champ Adresse de la passerelle, saisissez 0.0.0.0

16. Dans le champ Type ID, sélectionnez Nom unique.

    Il n'est pas nécessaire de fournir d'ID phase, car le Firewall/VPN Symantec recherche automatiquement les identifications d'utilisateur correspondantes dans sa base de données.

17. Cliquez sur **Ajouter**.

Le côté Firewall/VPN 200R Symantec du tunnel est à présent configuré.

## Configuration du Client Symantec Enterprise VPN pour un tunnel dynamique vers le Firewall/VPN 200R Symantec

Le tableau suivant indique les étapes requises pour configurer le Client Symantec Enterprise VPN pour un tunnel dynamique vers le Firewall/VPN 200R Symantec. Pour plus d'informations, consultez le Guide de l'administrateur du Client Symantec Enterprise VPN.

**Table 8-1 : Configuration du Client Symantec Enterprise VPN**

| Etapes de configuration | Guide de configuration du Client Symantec Enterprise VPN Chapitre - Section - Sous-section |
|---|---|
| 1. Lancer le Client Symantec Enterprise VPN. | Getting Started |
| 2. Créer une nouvelle passerelle. | Managing Gateways - Adding a Gateway |
| 3. Indiquez l'adresse externe (ou le nom DNS) du Firewall/VPN 200R Symantec. | Managing Gateways - Adding a Gateway |
| 4. Désélectionnez le Firewall/ PowerVPN Symantec. | Managing Gateways - Adding a Gateway |
| 5. Indiquez le "secret partagé". | Managing Gateways - Adding a Gateway |
| 6. Indiquez l'ID client. | Managing Gateways - Adding a Gateway |
| 7. Créez une nouvelle politique IKE sous un nom unique ou utilisez l'une des politiques prédéfinies. | Managing Gateways - Adding a Gateway - Defining an IKE Policy |
| 8. Créer un nouveau tunnel. | Managing Tunnels - Adding a Tunnel |
| 9. Indiquez le sous-réseau interne du Firewall/VPN 200R Symantec. | Managing Tunnels - Adding a Tunnel |
| 10. Créez une nouvelle politique VPN ou utilisez une politique prédéfinie. | Managing Tunnels - Adding a Tunnel - Defining an VPN Policy |
| 11. Connecter un tunnel. | Managing Tunnels - Adding a Tunnel |

# Chapitre 9

# Dépannage

## Problème 1 : Impossible de se connecter au Firewall/VPN Symantec pour le configurer.

Vérifiez que :

- l'installation du Firewall/VPN Symantec est correcte, les connexions réseau fonctionnent et le Firewall/VPN Symantec est sous tension.
- votre PC et le Firewall/VPN Symantec sont sur le même segment de réseau. Si vous installez le Firewall/VPN Symantec pour la première fois, vérifiez que votre PC utilise une adresse IP faisant partie de la plage 192.168.0.2 à 192.168.0.255, compatible avec l'adresse IP par défaut du Firewall/VPN (192.168.0.1).
- le masque de sous-réseau est défini sur 255.255.255.0 pour pouvoir atteindre le Firewall/VPN. Dans Windows, examinez ces paramètres dans la section Réseau du Panneau de configuration pour vérifier les propriétés du protocole TCP/IP utilisé par votre carte réseau.
- vous n'avez pas de proxy configuré dans votre navigateur. Si un ordinateur est connecté directement au Firewall/VPN Symantec, vérifiez que vous utilisez un câble "direct" fourni avec l'unité ou acheté chez un revendeur.
- votre carte réseau est compatible 10/100BaseT.

## Problème 2 : Quand je saisis une URL ou une adresse IP, j'obtiens une erreur de délai dépassé.

Essayez les méthodes de dépannage suivantes :

- Vérifiez si d'autres ordinateurs fonctionnent avec la même URL. Si c'est le cas, vérifiez que les paramètres IP de votre ordinateur sont corrects (adresse IP, masque de sous-réseau, passerelle par défaut et DNS).

- Vérifiez que la plage IP que vous utilisez n'est pas utilisée par un fournisseur de service (192.168.X.X ou 10.X.X.X). Si les autres ordinateurs ne peuvent pas se connecter non plus, vérifiez que vous avez connecté le Firewall/VPN Symantec correctement, décrit dans la section Installation.

- Si le Firewall/VPN Symantec est configuré correctement, vérifiez que votre connexion Internet (xDSL/modem câble, etc…) fonctionne quand elle est branchée directement sur votre ordinateur.

## Problème 3 : Certaines applications ne fonctionnent pas correctement avec le Firewall/VPN.

Utilisez l'écran Applications spéciales pour autoriser l'utilisation d'applications Internet spéciales.

- Le Firewall/VPN Symantec traite les données qui le traverse, il n'est donc pas transparent. L'application peut avoir besoin que certains ports TCP et UDP soient libérés pour fonctionner correctement. Consultez le site Web de l'éditeur pour savoir comment utiliser l'application derrière un firewall.

- Si vous avez toujours un problème, vous pouvez utiliser la fonction Hôte exposé. Elle devrait fonctionner avec la plupart des applications, mais elle constitue un risque de sécurité, car le firewall est désactivé pour le PC exposé et un seul PC peut l'utiliser. Quand la fonctionnalité Hôte exposé est utilisée, il est recommandé de désactiver les fonctionnalités Applications spéciales et Serveur virtuel.

## Problème 4 : L'authentification PPPoE échoue.

PPPoE n'est peut-être pas configuré correctement ou vous devez peut-être mettre à niveau votre micrologiciel. Vérifiez les points suivants :

- Veillez à cliquer sur le bouton **Enregistrer** après avoir saisi des informations dans l'écran d'installation PPPoE.
- Le nom d'utilisateur et le mot de passe doivent être saisis exactement tels qu'ils vous ont été indiqués par votre fournisseur (majuscules/minuscules). Le suffixe de nom de service peut être nécessaire pour se connecter. Vérifiez auprès de votre fournisseur que vous utilisez le nom d'utilisateur et le mot de passe corrects ainsi que tous les suffixes nécessaires.
- Vous pouvez essayer de saisir votre nom d'utilisateur suivi du caractère "@" et du domaine de votre fournisseur de service. Exemple : John@sympatico.ca Si votre fournisseur prend en charge des services, le bouton Obtenir services sur l'écran PPPoE avancé aura le même effet, sans avoir besoin de suffixe.

# Chapitre 10

# Mises à niveau du micrologiciel

Le Firewall/VPN Symantec effectue sa tâche en suivant une série d'instructions codées dans sa mémoire permanente. Ces instructions sont désignées "micrologiciel". Le micrologiciel contient toutes les fonctionnalités du Firewall/VPN.

Les mises à niveau du micrologiciel sont disponibles sur le site Web de Symantec. La version courante du micrologiciel est affichée dans l'écran Statut de l'interface. Si cette version est antérieure à celle présente sur le site Web, vous pouvez télécharger ce micrologiciel pour mettre à jour votre Firewall/VPN Symantec.

Les procédures suivantes considèrent que l'adresse IP de l'unité est la valeur par défaut (192.168.0.1). Si ce n'est pas le cas, substituez l'adresse correcte dans les instructions.

La mise à niveau du micrologiciel peut effacer vos paramètres de configuration (ce n'est généralement pas le cas, mais certains micrologiciels peuvent avoir cet effet). Veuillez à noter tous vos paramètres avant de procéder à la mise à niveau du micrologiciel. N'utilisez pas le fichier de sauvegarde d'une configuration de micrologiciel antérieure pour restaurer vos paramètres.

Pour effectuer la mise à niveau, vous avez besoin du micrologiciel téléchargé depuis le site Web de Symantec et de l'utilitaire nxtftp, disponible sur le CD, dans le dossier Utilities (il y a une commande pour Windows et une commande pour DOS ; nous utiliserons ici la commande DOS). Placez l'utilitaire nxtftpw et le nouveau micrologiciel dans un dossier temporaire sur votre disque dur.

**Remarque :** Si votre ordinateur n'est pas sous Windows, vous pouvez utiliser la commande TFTP de cet ordinateur, configurée en mode binaire, pour effectuer la même procédure (TFTP est relativement universel et disponible sous Macintosh, Unix, Linux, etc...).

## Pour mettre à niveau le micrologiciel

1. Coupez l'alimentation de l'unité en débranchant le câble électrique à l'arrière du Firewall/VPN.

2. Basculez les micro-commutateurs 1 et 2 en position **ON** (VERS LE BAS).

3. Réinsérez le connecteur d'alimentation dans la prise du Firewall/VPN Symantec.

4. Ouvrez une fenêtre DOS en cliquant sur Démarrer puis sur Exécuter… Saisissez la commande et cliquez sur **OK**.

5. Avec la commande CD, passez dans le répertoire temporaire contenant le micrologiciel et l'utilitaire nxtftp.

6. Saisissez nxtftp 192.168.0.1 PUT <nom du micrologiciel> et appuyez sur **Entrée**.

7. Après quelques instants, vous devrez voir apparaître un message indiquant la réussite de l'opération. Si ce n'est pas le cas redémarrez l'ordinateur et réessayez.

8. Remettez les micro-commutateurs dans leur position normale.

# Index

## V

# *Support technique*

Faisant partie intégrante de l'équipe d'experts de Symantec Security Response, notre support technique mondial gère les centres de support à travers le monde. Notre objectif premier est de répondre aux questions spécifiques sur les fonctionnalités/fonctions, l'installation et la configuration de nos produits ainsi que sur le contenu de notre Base de connaissances accessible par le Web. Pour répondre à vos questions en un temps record, nous travaillons en collaboration avec les autres services fonctionnels de Symantec comme avec notre service Ingénierie produit (Product Engineering) et nos Centres de recherche sur la sécurité (Security Research Centers) afin de fournir des Services d'alertes et des Mises à jour des définitions de virus pour les derniers Virus découverts et les Alertes de sécurité.

**Caractéristiques de nos offres :**

- Une panoplie d'options de support vous permet de choisir le service approprié pour n'importe quel type d'entreprise.
- Le support Web et téléphonique fournit des réponses rapides et des informations de dernière minute.
- Une garantie logicielle fournit une protection de mise à niveau logicielle automatique.
- Les Mises à jour de contenu des définitions de virus et les signatures de sécurité assurent la meilleure protection.
- Le support mondial composé d'experts Symantec est disponible 24h/24, 7j/7 dans le monde entier et dans différentes langues.
- Les fonctionnalités avancées telles que le Service d'alertes Symantec (Symantec Alerting Service) et le Responsable de compte technique (Technical Account Manager) offrent un support d'intervention et de sécurité proactive.

Rendez-vous sur notre site Web pour obtenir les dernières informations sur les programmes de support.

## Enregistrement et licences

Si le produit que vous mettez en œuvre requiert un enregistrement et/ou une clé de licence, la façon la plus simple et la plus rapide d'enregistrer votre service est d'accéder à notre site d'enregistrement et de licences à l'adresse suivante : www.symantec.com/certificate (en anglais). Vous pouvez également vous rendre sur le site Web www.symantec.fr/frsupport/, sélectionner le produit que vous souhaitez enregistrer et, à partir de la page d'accueil du produit, sélectionnez le lien d'enregistrement et de licences.

## Coordonnées du support

Les clients disposant d'un contrat de support en cours peuvent contacter le Support technique par téléphone ou sur le site Web à l'adresse suivante : http://www.symantec.fr/frsupport/.

**Lorsque vous contactez le support technique, vérifiez que vous disposez des informations suivantes :**

- La version du produit
- Les informations sur le matériel
  - La mémoire disponible, l'espace disque et la carte d'interface réseau
- Le système d'exploitation
  - La version et le correctif
- La typologie du réseau
  - Le routeur, la passerelle et l'adresse IP
- La description du problème
- Les messages d'erreur/les fichiers journaux
- Le type de réparation effectué avant de contacter Symantec
- Les modifications de réseau et/ou de configuration logicielle récentes

## Service clientèle

Contactez le Service clientèle Enterprise en ligne à l'adresse suivante : http://www.symantec.fr, sélectionnez le site de votre pays, puis choisissez « Service et Support ». Le Service clientèle est disponible pour résoudre les types de problèmes suivants :

- Les questions sur les licences et la sérialisation des produits
- La mise à jour d'enregistrement de produits avec changement de nom et d'adresse
- Les questions d'avant vente non techniques
- Les brochures produits
- L'absence ou le remplacement de manuels, disquettes ou CD-ROM défectueux
- Les commandes de mise à niveau